

# **Informationelle Selbstbestimmung - ein Grundrecht im Wandel?**

Dissertation  
der Rechtswissenschaftlichen Fakultät  
der Universität Zürich

zur Erlangung der Würde einer Doktorin der Rechtswissenschaft

vorgelegt von

**Stefanie-Daniela Waldmeier**

von Basel BS

genehmigt auf Antrag von

Prof. Dr. Thomas Gächter  
und  
Prof. Dr. Beat Rudin

Die Rechtswissenschaftliche Fakultät gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin angesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 20. Mai 2015

Die Dekanin: Prof. Dr. Christine Kaufmann

Die Dissertation ist als Internetpublikation auf der Homepage der Zentralbibliothek Zürich erschienen [www.zb.uzh.ch](http://www.zb.uzh.ch)

Zürich, 2015

## **Vorwort und Dank**

Die vielen privaten, aber auch geschäftlichen Diskussionen zum Thema Privatsphäre im digitalen Zeitalter sowie das Bedürfnis nach Antworten auf die Fragen, ob bzw. weshalb ein Grundrecht auf informationelle Selbstbestimmung notwendig ist, was informationelle Selbstbestimmung eigentlich bedeutet und wie sie ggf. besser umgesetzt werden könnte, veranlassten mich zur Erforschung dieses elementaren Rechts. Dabei erhebt die vorliegende Arbeit keineswegs den Anspruch, diese Fragen endgültig und unter Beachtung sämtlicher Aspekte zu beantworten. Vielmehr sehe ich ihren Sinn und Zweck darin, für die Klärung der aufgeworfenen Fragen etwas tiefer zu graben und nach dem wirklichen Wert dieses Grundrechts für die Allgemeinheit zu forschen. Wenn dann mit den dargestellten Lösungsansätzen ein Anstoss für die dringend notwendige Diskussion um den Erhalt dieses Grundrechts und das dadurch geschützte Gut gegeben werden kann, ist meinem Anliegen bereits Genüge getan.

Zweifelsohne wäre die Ausarbeitung der vorliegenden Dissertation ohne die Unterstützung einer Vielzahl von Personen kaum möglich gewesen. Deshalb an dieser Stelle ein herzliches Dankeschön für die liebevolle Unterstützung auf meinem bisherigen Weg und für das stete Gefühl getragen zu werden an Christian, meine Eltern und Freunde, ohne euch wäre ich nicht da, wo ich heute bin. Speziell bedanken möchte ich mich bei Svenja und Sandra für die Ermutigungen und die kritische Durchsicht, bei Markus für das nervenraubende In-Form-bringen sowie bei meinen Begutachtern, welche mir durch die Gelegenheit eine Dissertation zu verfassen, die Chance gaben, meinen Horizont zu erweitern und mich auf Unbekanntes einzulassen.

Basel, im Juli 2015

Stefanie-Daniela Waldmeier

## **Inhaltsverzeichnis**

Inhaltsverzeichnis .....	I
Abkürzungsverzeichnis.....	VI
Literaturverzeichnis .....	X
Materialienverzeichnis .....	XIX

## **I EINLEITUNG..... 1**

## **II GESCHICHTLICHER ABRISS BIS ZUR AUFNAHME IN DIE BV VON 1999.... 3**

1 The right to be let alone – Schutz der Privatsphäre .....	3
2 Konzeption eines Rechts auf informationelle Selbstbestimmung .....	6
3 Übernahme und Entwicklung durch das deutsche Bundes-verfassungsgericht.....	6
4 Adaption durch das Bundesgericht .....	8
5 «Eingang» in die neue Bundesverfassung .....	10
6 Résumé und Überleitung .....	11

## **III UMSETZUNG IN RECHTSPRECHUNG, LEHRE UND BUNDESRECHT ..... 12**

1 (Weitere) höchstrichterliche Auseinandersetzung .....	12
1.1 Konkretisierungsschwierigkeiten.....	12
1.2 Neuere Entscheide – Selbstbestimmung tritt in den Hintergrund .....	13
1.3 Fazit.....	15
2 Bundesgesetzgeberische Auseinandersetzung .....	15
2.1 Das DSG .....	16
2.1.1 Die Idee .....	16
2.1.2 Der Gesetzestext.....	18
2.1.2.1 Bearbeiten von Personendaten durch Privatpersonen .....	18
2.1.2.2 Bearbeiten von Personendaten durch Bundesorgane .....	20
2.1.2.3 Der EDÖB .....	23
2.1.3 Fazit .....	24
2.2 Art. 179 ff. StGB - Strafbare Handlungen gegen den Geheim- oder Privatbereich .....	25
2.2.1 Art. 179 StGB – Verletzung des Schriftgeheimnisses .....	25
2.2.2 Art. 179 <sup>bis</sup> StGB – Abhören und Aufnahmen fremder Gespräche .....	26
2.2.3 Art. 179 <sup>ter</sup> StGB – Unbefugtes Aufnehmen von Gesprächen .....	27

## Inhaltsverzeichnis

2.2.4	Art. 179 <sup>quater</sup> StGB – Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte .....	28
2.2.5	«Relativierung» und Rechtfertigungsgründe .....	29
2.2.6	Fazit .....	29
2.3	Fazit .....	30
<b>3</b>	<b>Auseinandersetzung in der Lehre .....</b>	<b>31</b>
3.1	Schutzzweck .....	32
3.2	Grundrechtsträger .....	33
3.3	Sachlicher Schutzbereich .....	34
3.3.1	Schutzobjekt .....	34
3.3.2	Schutzumfang .....	37
3.4	Kerngehalt .....	39
3.5	Fazit .....	42
<b>4</b>	<b>Résumé und Überleitung .....</b>	<b>42</b>
<b>IV</b>	<b>KRITIK AM HERRSCHENDEN VERSTÄNDNIS UND DEREN WÜRDIGUNG .....</b>	<b>44</b>
<b>1</b>	<b>Herkunft – Unterschied zwischen der deutschen und der schweizerischen Rechtsordnung .....</b>	<b>44</b>
<b>2</b>	<b>Konturlosigkeit und Inhaltsleere .....</b>	<b>45</b>
<b>3</b>	<b>Ein de facto-Informationsverbot .....</b>	<b>46</b>
<b>4</b>	<b>Grundrechtskollision / Verletzung des Grundsatzes der Gleichrangigkeit der Grundrechte .....</b>	<b>48</b>
<b>5</b>	<b>Realisierbarkeit .....</b>	<b>50</b>
<b>6</b>	<b>Ist Selbstbestimmung in Bezug auf Informationen überhaupt möglich? .....</b>	<b>52</b>
6.1	Was ist Selbstbestimmung? .....	53
6.1.1	Errungenschaft der Aufklärung .....	53
6.1.2	Grundvoraussetzung menschlicher Interaktion .....	54
6.1.3	Mensch als vernunftbegabtes Wesen .....	55
6.1.4	Alltagspsychologisches System .....	56
6.1.5	Voraussetzungen .....	57
6.1.6	Fazit .....	60
6.2	Was sind Informationen? .....	60
6.2.1	Kein einheitlicher Begriff – kein einheitliches Konzept .....	60
6.2.2	Informationen als Vorgang, Zustand, Inhalt .....	61
6.2.3	Information als Inhalt versus Inhalt der Information .....	62

## Inhaltsverzeichnis

6.2.4	Definitionsversuch .....	63
6.2.5	Fazit .....	64
6.3	Was sind Daten? .....	64
6.4	Gibt es ein Selbstbestimmungsrecht bezüglich Informationen/Daten? .....	66
6.4.1	Selbstbestimmung bezüglich Personeninformationen .....	66
6.4.2	Selbstbestimmung bezüglich Personendaten .....	67
6.5	Fazit.....	68
7	Résumé und Überleitung .....	69
<b>V</b>	<b>SCHUTZBEDARFSANALYSE .....</b>	<b>71</b>
1	Alltagssituationen und gesellschaftliche Konventionen .....	71
2	Informationelle Privatheit und deren Verletzung .....	71
3	Informationen und Daten prägen Rollen und Beziehungen.....	72
4	Enttäuschte Erwartungen .....	74
5	Die Konsequenzen .....	76
5.1	Angepasstes Verhalten .....	76
5.2	Steigende Tendenz bei Manifestation.....	77
6	Private «Räume» als essentielle Voraussetzung .....	80
7	Informationen und Daten brauchen keine Relation in der Realität .....	82
8	Nicht jede Information, jedes Personendatum schützenswert? .....	85
8.1	Kategorisierung von Daten.....	85
8.2	5-Elemente-These.....	86
9	Résumé und Überleitung .....	89
<b>VI</b>	<b>VORSCHLÄGE ZUR STÄRKUNG DES RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG .....</b>	<b>91</b>
1	Bessere Konturierung der relevanten Grundrechte .....	91
1.1	Privatsphäre oder persönliche Freiheit? .....	92
1.1.1	Das Zwiebelmodell .....	92
1.1.2	Privatheit – Privacy.....	95
1.2	Art. 13 Abs. 2 BV - Schutz vor Missbrauch persönlicher Daten .....	98
1.3	Zusammenführung und Würdigung .....	100

## Inhaltsverzeichnis

1.3.1	Wenige Überlappungen – kohärenterer Grundrechtsschutz.....	100
1.3.2	Missbrauchsschutz reicht nicht .....	101
1.3.3	Fazit.....	104
<b>2</b>	<b>Unmittelbare Wirkung zwischen Privatpersonen.....</b>	<b>104</b>
2.1	Direkte Horizontalwirkung .....	105
2.2	Indirekte Horizontalwirkung.....	108
2.3	Fazit.....	108
<b>3</b>	<b>Parallelen zu anderen Rechten .....</b>	<b>109</b>
3.1	Annäherung an das sachenrechtliche Eigentum .....	109
3.1.1	Ausdehnung des Sachbegriffs .....	109
3.1.2	Analoge Anwendbarkeit .....	111
3.1.3	Fazit.....	113
3.2	Daten als Immaterialgüter .....	114
3.2.1	Definition und Gemeinsamkeiten .....	114
3.2.2	Analoge Anwendbarkeit des URG?.....	115
3.2.2.1	Der Werkbegriff .....	116
3.3	Fazit und Überleitung .....	119
<b>4</b>	<b>Revision und Interpretation DSG sowie Kompetenzerweiterung des EDÖB .....</b>	<b>120</b>
4.1	Revision DSG.....	120
4.1.1	Paradigmawechsel mit Revision von Art. 12 DSG .....	120
4.1.2	Revision Art. 3 lit. a DSG.....	122
4.1.3	Interpretation «Bearbeiten» nach Art. 3 lit. e DSG.....	123
4.2	Kompetenzerweiterung des EDÖB .....	125
4.3	Fazit.....	127
<b>5</b>	<b>Wirksame Selbstregulierung.....</b>	<b>128</b>
5.1	Herabsenkung prozessualer Risiken .....	128
5.1.1	Stärkung des kollektiven Rechtsschutzes .....	130
5.1.1.1	Klagemöglichkeiten .....	130
5.1.1.2	Prozesskosten.....	132
5.1.1.3	Beweisschwierigkeiten .....	133
5.1.2	Herabsetzung der prozessualen Risiken für die Einzelperson .....	134
5.1.3	Fazit.....	136
5.2	Herausgabe vermögenswerter Vorteile .....	136
5.2.1	Right of Publicity in den USA .....	136
5.2.2	Vermögenswerte Persönlichkeitsrechte in Deutschland .....	138
5.2.3	Vermögenswerte Persönlichkeitsrechte in der Schweiz .....	138
5.2.4	Fazit.....	140
5.3	Fazit.....	140

## Inhaltsverzeichnis

<b>6</b>	<b>Résumé und Überleitung .....</b>	<b>141</b>
<b>VII</b>	<b>PRAXISSTUDIE .....</b>	<b>143</b>
<b>1</b>	<b>Datenfluss im USB .....</b>	<b>143</b>
1.1	Klinikinformationssystem und Krankengeschichte.....	143
1.2	Seelsorger .....	144
1.3	Studie .....	144
<b>2</b>	<b>Datenfluss an Externe.....</b>	<b>145</b>
2.1	Nachbehandelnder Arzt .....	145
2.2	Krankenkasse .....	146
2.3	Bereich Gesundheitsversorgung des Gesundheitsdepartements Basel-Stadt.....	151
2.4	Kantonsarzt .....	151
2.5	Krebsregister beider Basel.....	153
2.6	Staatsarchiv Basel-Stadt.....	154
2.7	Zentrale Statistikstelle Basel-Stadt .....	154
2.8	Übersicht über die beschriebenen Datenflüsse .....	155
<b>3</b>	<b>Résumé.....</b>	<b>157</b>
<b>VIII</b>	<b>SCHLUSSWORT.....</b>	<b>159</b>
	Stichwortverzeichnis .....	161



## Abkürzungsverzeichnis

### **Abkürzungsverzeichnis**

a. M.	anderer Meinung
Abs.	Absatz
AcP	Archiv für civilistische Praxis, Tübingen
AJP	Aktuelle juristische Praxis, Lachen
AHV	Alters- und Hinterbliebenenversorgung
AmtBull	Amtliches Bulletin
Art.	Artikel
ArchivG	Gesetz (des Kantons Basel-Stadt) vom 11. September 1996 über das Archivwesen, SG 153.600
Aufl.	Auflage
BAG	Bundesamt für Gesundheit
Bd	Band
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BDSG	(Deutsches) Bundesdatenschutzgesetz vom 20. Dezember 1990
BGE	Amtliche Sammlung der Entscheidungen des Schweizerischen Bundesgerichts
BGH	(Deutscher) Bundesgerichtshof
BR	Bundesrat
BStatG	Bundesstatistikgesetz vom 9. Oktober 1992, SR 431.01
BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs, SR 780.1
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BVerfGE	Entscheidungen des (deutschen) Bundesverfassungsgerichts
CC	Code Civil (=ZGB)
CT	Computertomographie
digma	Zeitschrift für Datenrecht und Informationssicherheit, Zürich
Diss.	Dissertation
DNA	Desoxyribonukleinsäure (=Träger der Erbinformationen)
Dr.	Doktor
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1

## Abkürzungsverzeichnis

DuD	Datenschutz und Datensicherheit, Wiesbaden
E.	Erwägung(en)
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSB	Eidgenössische/r Datenschutzbeauftragte/er
EDV	Elektronische Datenverarbeitung
EMRK	Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten, SR 0.101
engl.	englisch
EpG	Bundesgesetz vom 18. Dezember 1970 über die Bekämpfung übertragbarer Krankheiten des Menschen, SR 818.101
et al.	et alii, et aliae
etc.	et cetera
EU	Europäische Union
EU-Datenschutzgrundverordnung	Verordnung des europäischen Parlaments und des Rates vom 25. Januar 2012 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
evt.	eventuell
f., ff.	folgende, fortfolgende
FN	Fussnote(n)
GesG	Gesundheitsgesetz (des Kantons Basel-Stadt) vom 21. September 2011, SG 300.100
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949
ggf.	gegebenenfalls
Habil.	Habilitation
HFG	Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, SR 810.30
HIV	Humanes Immundefizienz-Virus
Hrsg.	Herausgeber
i.S.v.	im Sinne von
IT	Informationstechnik
IV	Invalidenversicherung

## Abkürzungsverzeichnis

IVG	Bundesgesetz vom 19. Juni 1959 über die Invalidenversicherung
i.V.m.	in Verbindung mit
IDG	Gesetz (des Kantons Basel-Stadt) vom 9. Juni 2010 über die Information und den Datenschutz, SG 153.260
Jg	Jahrgang
KV	Verfassung des Kantons Basel-Stadt vom 23. März 2005, SG 111.10
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung, SR 832.10
KVV	Verordnung vom 27. Juni 1995 über die Krankenversicherung, SR 832.102
lit.	litera/literae
mbH	mit beschränkter Haftung
Melde-VO	Verordnung vom 13. Januar 1999 über die Meldung übertragbarer Krankheiten des Menschen, SR 818.141.1
m.w.H.	mit weiteren Hinweisen
m.w.Verw.	mit weiteren Verweisen
N	Note(n)
NR	Nationalrat
o.ä.	oder ähnlichem
ÖSpG	Gesetz vom 16. Februar 2011 über die öffentlichen Spitäler des Kantons Basel-Stadt, SG 331.100
OR	Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220
Prof.	Professor
RZ	Randziffer(n)
S.	Seite(n)
SFr.	Schweizer Franken
SG	Systematische Gesetzessammlung Basel-Stadt
sog.	sogenannte(r)
SR	Systematische Gesetzessammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311

## Abkürzungsverzeichnis

u.a.	unter anderem
URG	Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte, SR 231.1
vgl.	vergleiche
VHS	Video Home System (= Videobandsystem)
VO des EDI über Arzt- und Labormeldun- gen	Verordnung des EDI vom 13. Januar 1999 über Arzt- und Labormeldungen, SR 818.141.11
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210
Ziff.	Ziffer(n)
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008, SR 272

## Literaturverzeichnis

### Zitierweise:

Die nachstehenden Werke werden, soweit nichts anderes angegeben ist, mit Nachnamen des Autors sowie mit Seitenzahl, Randziffer oder Randnote zitiert, je nachdem, welche Angabe die Fundstelle am genauesten vermerkt.

- AEBI-MÜLLER REGINA E. Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005
- AENIS LORENZ/MÜHLEMANN DAVID Zur Qualifikation von E-Mails als Urkunde, in: digma 2013, Bd 4, S. 164 ff.
- ALBERS MARION Umgang mit personenbezogenen Informationen und Daten, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Assmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd 2, 2. Aufl., München 2012, S. 107 ff. (zit. Albers, Umgang)
- DIESELBE Informationelle Selbstbestimmung, Habil. Berlin 2001/2002, Baden-Baden 2005 (zit. Albers, Informationelle Selbstbestimmung)
- AMELUNG ULRICH Der Schutz der Privatheit im Zivilrecht: Schadensersatz und Gewinnabschöpfung bei Verletzung des Rechts auf informationelle Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht, Diss. Regensburg 2001, Tübingen 2002
- APERJIS CHRISTINA/HUBERMAN BERNARDO A. A Market for Unbiased Private Data: Paying Individuals According to their Privacy Attitudes, HP Social Computing Research, <<http://www.hpl.hp.com/research/scl/papers/datamarket/datamarket.pdf>> (zuletzt besucht am 7.2.2014)
- AUBERT JEAN-FRANÇOIS/MAHON PASCAL Petit commentaire de la Constitution fédérale suisse du 18 avril 1999, Zürich 2003
- BAERISWYL BRUNO «Big Data» ohne Datenschutz-Leitplanken, in: digma 2013, Bd 1, S. 14 ff. (zit. Baeriswyl, «Big Data»)
- DERSELBE Kleingedrucktes unter der Lupe, in: digma 2010, Bd 2, S. 56 ff. (zit. Baeriswyl, Kleingedrucktes)
- BARTH JOHN The end of the road, 1981
- BENN STANLEY A Theory of Freedom, in: Cambridge University Press 1988, Cambridge 1988
- BELSER EVA MARIA Zur rechtlichen Tragweite des Grundrechts auf Datenschutz, Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser

## Literaturverzeichnis

- (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013, S. 19 ff. (zit. Belser, Instrumente)
- BELSER EVA MARIA/  
EPINEY ASTRID/  
WALDMANN BERNHARD (HRSG.)      Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011 (zit. Autor, Datenschutzrecht, § ... N ...)
- BEUTHIEN VOLKER      Was ist vermögenswert, die Persönlichkeit oder das Image?, NJW 2003, 1220 ff. (zit. Beuthien, NJW, 2003)
- DERSELBE      Schützt das allgemeine Persönlichkeitsrecht auch kommerzielle Interessen der Person?, in: Volker Beuthien (Hrsg.), Persönlichkeitsgüterschutz vor und nach dem Tode, Marburger Medienschriften Bd 4, Baden-Baden 2002, 75 ff. (zit. Beuthien, Persönlichkeitsrecht).
- BEUTHIEN VOLKER/  
SCHMÖLZ ANTON S.      Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, Erlösherausgabe statt nur billige Entschädigung in Geld, Schriftreihe Information und Recht, Bd 5, München 1999
- BIAGGINI GIOVANNI      Bundesverfassung der Schweizerischen Eidgenossenschaft, Zürich 2007 (zit. Biaggini, N ... zu Art. ... BV)
- BIENE DANIEL      Starkult, Individuum und Persönlichkeitsgüterrecht, Diss. Zürich, Bern 2004.
- BONDOLFI ALBERTO      Zur «Privatsphäre» in sozialetischer Sicht: Einige Grundsatzüberlegungen zur ethischen Dimension des Datenschutzes, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, S. 127 ff.
- BRUNNER STEPHAN C.      Mit rostiger Flinte unterwegs in virtuellen Welten?, in: Jusletter vom 4. April 2011
- BRÜCKNER CHRISTIAN      Das Personenrecht des ZGB, Zweiter Teil, Der Schutz der Persönlichkeit, <<http://www.cbrueckner.ch/ccount/click.php?id=52>> (zuletzt besucht am 14. Juni 2014)
- BÜCHLER ANDREA      Die Kommerzialisierung von Persönlichkeitsgütern, Zur Dialektik von Ich und Mein, AcP 206 (2006), S. 300 ff.
- BULL HANS PETER      Informationelle Selbstbestimmung – Vision oder Illusion?, Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, 2. Aufl., Tübingen 2011 (zit. Bull, Informationelle Selbstbestimmung)
- DERSELBE      Datenschutz oder: Die Angst vor dem Computer, München 1984, (zit. Bull, Datenschutz)
- BURKERT HERBERT      Aktuelle Herausforderungen des Datenschutzrechts im Kontext nationaler und internationaler Entwicklungen, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur

## Literaturverzeichnis

- Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013, S. 19 ff.
- COOLEY THOMAS  
MCINTYRE A treatise on the law of torts, 2 Aufl., Callaghan 1888
- DIGGELMANN OLIV-  
VER Grundrechtsschutz der Privatheit, in: Veröffentlichungen der  
Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL)  
(Hrsg.), Der Schutzauftrag des Rechts, Berlin 2011, S. 50 ff.
- DENNINGER ER-  
HARD Das Recht auf informationelle Selbstbestimmung und Innere  
Sicherheit, in: Andreas Von Schoeler (Hrsg.), Informationsge-  
sellschaft oder Überwachungsstaat?, Opladen 1986, S. 106 ff.
- DESSEMONTET  
FRANÇOISE Le droit à sa proper image: Droit de la personnalité ou droit à la  
publicité, in: Mélanges en l'honneur de Jacques-Michel Gros-  
sen, Basel/Frankfurt a.M. 1992, S. 41 ff.
- DRUEY JEAN NICO-  
LAS Information als Gegenstand des Rechts: Entwurf einer Grund-  
lage, Zürich 1995 (zit. Druey, Information)
- DERSELBE Von der strukturellen Schwäche des Personenschutzes im In-  
formationsrecht, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Per-  
spektive Datenschutz, Praxis und Entwicklungen in Recht und  
Technik, Zürich 2002, S. 143 ff. (zit. Druey, Strukturelle Schwä-  
che)
- EHRENZELLER  
BERNHARD/  
SCHINDLER BENJA-  
MIN/ SCHWEIZER  
RAINER J./ VALLEN-  
DER KLAUS A.  
(HRSG.) Die Schweizerische Bundesverfassung, Kommentar, 3. Aufl.,  
Zürich/Basel/Genf 2014 (zit. Bearbeiter, SG-Komm BV, N ... zu  
Art. ... BV)
- DIESELBEN Die Schweizerische Bundesverfassung, Kommentar, 2. Aufl.,  
Zürich/Basel/Genf 2008 (zit. Bearbeiter, SG-Komm BV 2008, N  
... zu Art. ... BV)
- ERNST WOLFGANG Sachenrecht in a nutshell, 2. Aufl., Zürich/St. Gallen 2013
- EVERS HANS-  
ULRICH Privatsphäre und Ämter für Verfassungsschutz, Berlin 1960
- FLÜCKIGER ALE-  
XANDRE L'autodétermination en matière de données personnelles: un  
droit (plus si) fondamental à l'ère digitale ou un nouveau droit  
de propriété, in: AJP 2013, S. 837 ff.
- FRIED CHARLES Privacy, in: Yale Law Journal 77 (1968), S. 475 ff.
- GÄCHTER THOMAS/  
EGLI PHILIPP Informationsaustausch im Umfeld der Sozialhilfe, Rechtsgut-  
achten zuhanden der Gesundheits- und Fürsorgedirektion des  
Kantons Bern, in: Jusletter vom 6. September 2010
- GÄCHTER THOMAS/ Einbettung ausgewählter Konzepte in das schweizerische Da-

## Literaturverzeichnis

- WERDER GREGORI      tenschutzrecht, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013, S. 87 ff.
- GARSTKA  
HANSJÜRGEN      Selbstdatenschutz, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, S. 159 ff.
- GAUS WILHELM      Dokumentations- und Ordnungslehre, Theorie und Praxis des Information Retrieval, 5. Aufl., Heidelberg 2005
- GERHARDT VOLKER    Selbstbestimmung, Das Prinzip der Individualität, Stuttgart 1999
- GIACOMETTI ZAC-  
CARIA      Schweizerisches Bundesstaatsrecht, Neubearbeitung der 1. Hälfte des gleichnamigen Werkes von F. Fleiner, Zürich 1965 (1945)
- GOLLE PHILIPPE     Revisiting the uniqueness of simple demographics in the US population, in: Proc. 5th ACM Workshop on Privacy in Electronic Society, 2006
- HAAB ROBERT/ SI-  
MONIUS AUGUST/  
SCHERRER WER-  
NER/ ZOBL DIETER    Zürcher Kommentar zum Schweizerischen Zivilgesetzbuch, Band IV, 2. Aufl., Zürich 1977
- HESS-ODONI URS     Die Herrschaftsrechte an Daten, Jusletter 17. Mai 2004
- HIMMELMANN  
BEATRIX      Über Grenzen der Selbstbestimmung, in: Jan-Christoph Heilinger/Colin King/Héctor Wittwer (Hrsg.), Individualität und Selbstbestimmung, Berlin 2009, S. 325 ff.
- KAISER MARKUS/  
RÜETSCHI DAVID     Immaterialgüterrecht in a nutshell, Zürich/St. Gallen 2009
- KAMP MEIKE/ ROST  
MARTIN      Kritik an der Einwilligung, Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, in: DuD 2013, Bd 2, S. 80 ff.
- KANT IMMANUEL      Beantwortung der Frage: Was ist Aufklärung?, in: Berlinische Monatsschrift, 2 (1784), S. 481 ff.
- KARG, MORITZ      Die Renaissance des Verbotsprinzips im Datenschutz, in: DuD 2013, Bd 2, S. 75 ff.
- DERSELBE      Der Wert personenbezogener Daten, in: digma 2011, Bd. 4, S. 146 ff.
- KARJOTH GÜNTHER    Sind anonymisierte Daten anonym genug?, in: digma 2008, Bd 1, S. 18 ff.
- KEYSSNER HUGO     Das Recht am eigenen Bilde, Diss. Berlin, Guttentag 1896
- KIENER REGINA/  
KÄLIN WALTER      Grundrechte, Bern 2007



## Literaturverzeichnis

- KRÄHNKE UWE            Selbstbestimmung, Zur gesellschaftlichen Konstruktion einer normativen Leitidee, Weilerswist 2007
- KRAMER ERNST A.        Juristische Methodenlehre, 2. Aufl., Bern 2005
- LABSCH KARL HEINZ     Staats- und Verwaltungsrecht, München 2007
- LESSIG LAWRENCE        CODE Version 2.0, New York 2006
- LOMBROSO CESARE        Der Verbrecher (homo delinquens) in anthropologischer, ärztlicher und juristischer Beziehung, Bände 1-2, Hamburg 1894
- LUHMANN NIKLAS         Grundrechte als Institution, ein Beitrag zur politischen Soziologie, Berlin 1965
- MAURER-LAMBROU  
URS/ BLECHTA  
GABOR P. (HRSG.)        Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. Bearbeiter, BaKomm DSG/BGÖ, N ... zu Art. ... DSG)
- MAURER-LAMBROU  
URS/ VOGT NEDIM  
PETER                        Basler Kommentar zum Datenschutzgesetz, 2. Aufl., Basel 2006 (zit. Bearbeiter, BaKomm DSG, N ... zu Art. ... DSG)
- MAYER-  
SCHÖNBERGER VIK-  
TOR/ CUKIER KEN-  
NETH                        Big Data: Die Revolution, die unser Leben verändert, 2. Aufl., München 2013
- MAYER-  
SCHÖNBERGER VIK-  
TOR                         Information und Recht, Vom Datenschutz bis zum Urheberrecht, Wien 2001
- MEYER CAROLINE  
B.                            Privatrechtliche Persönlichkeitsrechte im kommerziellen Rechtsverkehr, Eine rechtsvergleichende Untersuchung zur tatsächlichen und rechtlichen Kommerzialisierung von Persönlichkeitsrechten, Basel 2008
- MONNIER GILLES         Le piratage informatique en droit pénal, in: sic! 2009, S. 141 ff.
- MÜLLER JÖRG PAUL        Allgemeine Bemerkungen zu den Grundrechten, in: Daniel Thürer/Jean-François Aubert /Jörg Paul Müller (Hrsg.), Verfassungsrecht der Schweiz, Zürich 2001, S. 621 ff.
- MÜLLER JÖRG  
PAUL/ SCHEFER  
MARKUS                    Grundrechte der Schweiz, 4. Aufl., Bern 2008
- MÜLLER MARKUS         Individuelle Selbstbestimmung und staatliche Fürsorge, in: ZSR 131 (2012), S. 63 ff. (zit: Müller Markus, Selbstbestimmung)
- NIGGLI MARCEL  
ALEXANDER/  
WIPRÄCHTIGER  
HANS (HRSG.)            Basler Kommentar zum Strafrecht II, Art. 111-392 StGB, 2. Aufl., Basel 2007 (zit. Bearbeiter, BaKomm StGB, N ... zu Art. ... StGB)
- PASSADELIS NICO-        Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher

## Literaturverzeichnis

- LAS/ ROSENTHAL  
DAVID/THÜR  
HANSPETER  
(HRSG.) Verwaltung, Basel 2015 (zit. Bearbeiter, Datenschutzrecht, RZ)
- POLEDNA TOMAS/  
CODONI STEFANO Sanktionierung von Informationsrechtsverletzungen, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, S. 265 ff.
- POLZER GEORG Big data – eine Einführung, in: digma 2013, Bd 1, S. 6 ff.
- PÖTZL WALTER  
/HEYDENREUTER  
REINHARD/ KOHL-  
BERGER ALEXANDRA Mörder, Räuber, Hexen: Kriminalgeschichte des Mittelalters und der Frühen Neuzeit, Augsburg 2005
- PREISWERK VALEN-  
TIN Das Recht am eigenen Bild, Diss. Basel 1946
- PRINZ WOLFGANG Der Mensch ist nicht frei, Ein Gespräch, in: Christian Geyer (Hrsg.), Hirnforschung und Willensfreiheit, Zur Deutung der neuesten Experimente, Frankfurt am Main 2004, S. 20 ff.
- RHINOW RENÉ/  
SCHEFER MARKUS Schweizerisches Verfassungsrecht, 2. Aufl., Basel 2009
- RIKLIN FRANZ Der strafrechtliche Schutz des Rechts am eigenen Bild, in: Detlev-Christian Dicke/Thomas Fleiner-Gerster (Hrsg.), Staat und Gesellschaft, Festschrift für Leo Schürmann, Freiburg 1987, S. 535 ff.
- RITSERT JÜRGEN Bestimmung und Selbstbestimmung, Zur Idee der Freiheit, Hamburg 2007
- ROSENTHAL DAVID/  
JÖHRI YVONNE  
(HRSG.) Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008 (zit. Bearbeiter, Handkommentar DSG, N ... zu Art. ...)
- ROSENTHAL DAVID Projekt Internet, Was Unternehmen über Internet und Recht wissen müssen, Zürich 1997
- RÖSSLER BEATE Der Wert des Privaten, Frankfurt am Main 2001
- ROSSNAGEL ALE-  
XANDER Modernisierung des Datenschutzes, in: digma 2011, Bd. 4, S. 160 ff.
- RUDIN BEAT/  
BAERISWYL BRUNO  
(HRSG.) Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014 (zit. Bearbeiter, Praxiskommentar IDG, N ... zu § ...)
- RUDIN BEAT Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, in: SJZ 105 (2009) Nr. 1, S. 1 ff. (zit. Rudin, Verfassungswidrige Anwendbarkeit)

## Literaturverzeichnis

- DERSELBE Die Erosion der informationellen Privatheit, oder, Rechtsetzung als Risiko?, in: Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (Hrsg.), Risiko und Recht, Festgabe zum Schweizerischen Juristentag 2004, Basel 2004, S. 415 ff. (zit. Rudin, Erosion)
- DERSELBE Datenschutzaufsicht – vom Kontrolleur zum Kompetenzzentrum, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, S. 373 ff. (zit. Rudin, Datenschutzaufsicht)
- RUDOLF WALTER Recht auf informationelle Selbstbestimmung, in: Merten Detlef/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Band IV, Grundrechte in Deutschland: Einzelgrundrechte I, Heidelberg 2011, S. 233 ff.
- RUSCH ARNOLD Der Chevrolet Malibu, sein Tank und das «Ivey Memo», in: AJP 2014, S. 137 ff.
- SCHAAR PETER Das Ende der Privatsphäre, Der Weg in die Überwachungs-gesellschaft, München 2009
- SCHEFER MARKUS Grundrechtliche Schutzpflichten und die Auslegung staatlicher Aufgaben, in: AJP 2002, S. 1131 ff. (zit. SCHEFER, Schutzpflich-ten)
- DERSELBE Die Kerngehalte von Grundrechten, Geltung, Dogmatik, inhaltliche Ausgestaltung, Bern 2001 (zit. SCHEFER, Kerngehalte)
- SCHERTZ CHRIS-  
TIAN/ HÖCH DOMINIK Privat war gestern, Wie Medien und Internet unsere Werte zer-  
stören, Berlin 2011
- SCHMID JÖRG/  
HÜRLIMANN-KAUP  
BETTINA Sachenrecht, 2. Aufl., Zürich/Basel/Genf 2003
- SCHWANINGER DA-  
VID/ LATTMANN  
STEPHANIE S. Cloud Computing: Ausgewählte rechtliche Probleme in der  
Wolke, in: Jusletter vom 11. März 2013
- SCHWARZ GERHARD Privatheit – Sauerstoff der Freiheit, in: Konrad Humm-  
ler/Gerhard Schwarz (Hrsg.), Das Recht auf sich selbst, Be-  
drohte Privatsphäre im Spannungsfeld zwischen Sicherheit und  
Freiheit, Zürich 2003, S. 11 ff.
- SCHWEIZER RAINER  
J. Selbstbestimmung in der transparenten Gesellschaft, in: Kon-  
rad Hummler/Gerhard Schwarz (Hrsg.), Das Recht auf sich  
selbst, Bedrohte Privatsphäre im Spannungsfeld zwischen Si-  
cherheit und Freiheit, Zürich 2003, S. 93 ff.
- SCHWEIZER RAINER  
J./ BISCHOF SE-  
VERIN Der Begriff der Personendaten, in: digma 2011, Bd 4, S. 152 ff.
- SIGRIST MARTIN Staatsschutz oder Datenschutz?, Die Vereinbarkeit präventiver

## Literaturverzeichnis

- Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung, Zürich 2014
- SIMITIS SPIROS (HRSG.) Kommentar zum Bundesdatenschutzgesetz, 8. Aufl., Frankfurt 2014 (zit. Bearbeiter, Kommentar BDSG, N ... zu §. ... BDSG)
- SOFSKY WOLFGANG Verteidigung des Privaten, Eine Streitschrift, München 2009
- SPÜHLER KARL/ TENCHIO LUCA/ INFANGER DOMINIK (HRSG.) Basler Kommentar zur Schweizerischen Zivilprozessordnung, 2. Aufl., Basel 2013 (zit. Bearbeiter, BaKomm ZPO, N ... zu Art. ... ZPO)
- STEINMÜLLER WILHELM/ LUTTERBECK BERND/ MALLMANN C./ HARBORT U./KOLB G./ SCHNEIDER J. Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, <<http://www.scribd.com/doc/39398927/1971-Grundfragen-Datenschutz-BAD06-3826>> (zuletzt besucht am 14.3.2012) (zit. Steinmüller et al.)
- STRATENWERTH GÜNTER/ JENNI GUIDO Schweizerisches Strafrecht, Besonderer Teil I, Straftaten gegen Individualinteressen, 6. Aufl., Bern 2003
- SWEENEY LATANYA Uniqueness of Simple Demographics in the U.S. Population, LIDAPWP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh 2000
- THALER DANIEL Haftung zwischen Wettkampfsportlern, insbesondere beim Sportunfall und Dopingmissbrauch, Diss. Zürich 2001, Zürich 2002
- THIEL MARKUS Die "Entgrenzung" der Gefahrenabwehr, Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, Habil. Düsseldorf 2010, Tübingen 2011
- VAN SPYK BENEDIKT Das Recht auf informationelle Selbstbestimmung in der Humanforschung, Zugleich eine Untersuchung der Grundlagen und Grenzen des «informed consent» im Handlungsbereich der Forschung am Menschen, Zürich/St. Gallen 2011
- VOGELSANG KLAUS Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987
- WARREN SAMUEL D./ BRANDEIS LOUIS D. The Right to Privacy, in: Harvard Law Review 4 (1890), S. 193 ff.
- WENDT RUDOLF Der Garantiegehalt der Grundrechte und das Übermassverbot, Zur massstabsetzenden Kraft der Grundrechte in der Übermassprüfung, in: AöR 104 (1979), S. 414 ff.
- WERNER MARTIN Datenschutz in ortsbasierten Diensten, in: digma 2011, Bd 2, S. 54 ff.

## Literaturverzeichnis

- WESTIN ALAN      Privacy and Freedom, The Bodley Head, London/Sydney/Toronto 1967
- WIDMER BARBARA      Auftragsdatenbearbeitung - zum Zweiten, in: *digma* 2014, Bd 2, S. 76 ff.
- WILLASCHEK MARCUS      Der eigene Wille, in: Jan-Christoph Heilingner/Colin King/Héctor Wittwer (Hrsg.), *Individualität und Selbstbestimmung*, Berlin 2009, S. 91 ff.
- ZITTRAIN JONATHAN      What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, in: *Stanford Law Review* 52 (2000), 1201

## Materialienverzeichnis

### **Materialienverzeichnis**

Bericht BR	Bericht des Bundesrates vom 3. Juli 2013 über den kollektiven Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten
Regierungsratsbeschluss	Beschluss des Regierungsrates des Kantons Basel-Stadt vom 2. Dezember 2008, JD/085229
Botschaft über die Schaffung und die Anpassung gesetzlicher Grundlagen	Botschaft vom 25. August 1999 über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten, BBl 1999 9005 ff.
Botschaft BV	Botschaft vom 20. November 1996 über eine neue Bundesverfassung (BV), BBl 1997 1 ff.
Botschaft DSG	Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), BBl 1988 413 ff.

## I Einleitung

Das Recht auf informationelle Selbstbestimmung – alles kalter Kaffee oder hoch aktuell? Gerade im medizinischen Bereich fallen viele sehr sensible Daten und Informationen an. Besagten Daten und Informationen wird ein riesiger Erkenntnisgewinn zugesprochen, dies zum einen im Rahmen des Behandlungskontextes für die Einzelperson, auf die die jeweiligen Daten und Informationen verweisen (die sog. betroffene Person), im Rahmen von Forschung aber auch für die gesamte Menschheit. Dem medizinischen Interesse an diesen Daten und Informationen stehen jedoch nicht selten die Interessen der betroffenen Personen gegenüber. Obwohl gerade im Behandlungskontext auf den ersten Blick kaum ersichtlich ist, weshalb entgegenstehende Interessen bestehen sollten, sind solche auch und gerade hier nicht zu unterschätzen. Zu denken ist etwa an die Bekanntgabe solcher medizinischer Daten an die Krankenversicherungen, die diese zwar in erster Linie zwecks Vergütung der erbrachten Leistungen benötigen, die daraus gewonnenen Informationen aber auch dazu verwenden können, Leistungen an ein gewisses Verhalten zu binden. Von der Betroffenenenseite wird hier das Grundrecht auf informationelle Selbstbestimmung ins Felde geführt, welches dem einzelnen den Anspruch einräumen soll, selbst über die Verwendung seiner Daten zu bestimmen. Wer sich jedoch daran wagt herauszufinden, was der Schutzzweck dieses Grundrechts ist, wie sich sein Schutzbereich und Schutzobjekt definieren und was dessen Kernbereich sein soll, wird schnell feststellen, dass vieles unklar ist, dass solche Unklarheiten mit weitgefassten Formulierungen zu überdecken versucht werden oder dass sich gewisse von der Lehre getroffene Annahmen bei genauerer Betrachtung gar als falsch erweisen.

Das erste Ziel dieser Dissertation ist es deshalb, mit Hilfe eines bewusst kurz und wertungsfrei gehaltenen geschichtlichen Abrisses und einem Überblick über die Bemühungen zur Umsetzung und Konkretisierung dieses Grundrechts durch Gesetzgeber, Lehre und Rechtsprechung eine traditionelle Auslegung des Rechts auf informationelle Selbstbestimmung – so wie es heute mehrheitlich verstanden wird – zu erarbeiten. Nach dieser möglichst umfassenden Beleuchtung des vorherrschenden Verständnisses des Grundrechts werden die damit verbundenen Schwierigkeiten aufgezeigt und diskutiert. In diesem Zusammenhang ist auf das Wesen von Daten und In-

## I Einleitung

formationen einzugehen, und es muss der Frage nachgegangen werden, ob Selbstbestimmung in Bezug auf Informationen und Daten überhaupt möglich ist. Ausgehend von dieser Untersuchung folgt anschliessend eine Schutzbedarfsanalyse, die Aufschluss darüber geben soll, ob, und wenn ja, weshalb trotz der aufgezeigten Schwierigkeiten am Recht auf informationelle Selbstbestimmung festgehalten werden muss. Sodann wird eine Auswahl von Vorschlägen und Ideen vorgestellt und diskutiert, um dem aus der Schutzbedarfsanalyse resultierenden Ergebnis in der Praxis auch zu vermehrter Beachtung zu verhelfen. Abgeschlossen wird die Dissertation mit einer Praxisstudie, welche ausgehend von einem Anschauungsfall die bestehenden Datenflüsse im medizinischen Alltag beleuchtet und die potentiellen Veränderungen darauf durch das erarbeitete Verständnis eines Rechts auf informationelle Selbstbestimmung aufzeigt.



## **II Geschichtlicher Abriss bis zur Aufnahme in die BV von 1999**

Beim Grundrecht auf informationelle Selbstbestimmung handelt es sich nicht um eines jener rechtsstaatlichen Prinzipien, welche sich bereits aus der Naturrechtslehre ergeben haben und als solche immer schon Bestandteil rechtsstaatlicher Normkonzepte waren. Vielmehr wurde das der informationellen Selbstbestimmung zugrunde liegende Schutzgut erst im Laufe der Zeit mit der durch die *Industrialisierung* einhergehenden verdichteten Wohnsituation und der Entwicklung neuer Technologien, welche die *Perpetuierung von Daten* und deren *grossflächige Verteilung* ermöglichten, erahnt. Die Geschichte der informationellen Selbstbestimmung beginnt sodann erst mit dem gesellschaftlichen Zugeständnis eines privaten, persönlichen Bereichs und der Anerkennung eines rechtlichen Anspruchs auf Schutz eines solchen Bereichs. Erst aufgrund dieser Basis konnte die Entwicklung hin zu einem Recht in Bezug auf den Umgang mit persönlichen Daten und Informationen stattfinden.

Im Folgenden wird es darum gehen, die einzelnen Eckpunkte auf dem Weg bis hin zur bundesgerichtlichen Anerkennung eines Rechts auf informationelle Selbstbestimmung und zur «Aufnahme» in die Bundesverfassung darzustellen sowie die damit einhergegangenen Schwierigkeiten aufzuzeigen.

### **1 The right to be let alone – Schutz der Privatsphäre**

Moderne Informationsbeschaffungs- und Informationsverbreitungsmittel führten im 19. Jahrhundert dazu, dass sich die Menschen in industrialisierten Ländern immer häufiger in ihrem privaten Bereich beeinträchtigt fühlten. In den USA haben fotografische Aufnahmen privater Szenen in Verbindung mit den Geschäftsmethoden der Klatschpresse die beiden Anwälte Samuel D. Warren und Louis D. Brandeis 1890 veranlasst, einen Aufsatz zu veröffentlichen, in dem sie das Recht auf Privatheit als «the right to be let alone» postulierten.<sup>1</sup> Diese markante Formulierung stammt ur-

---

<sup>1</sup> WARREN/BRANDEIS, S. 193 ff.

## II Geschichtlicher Abriss bis zur Aufnahme in die BV von 1999

sprünglich von Richter Thomas McIntyre Cooley, der sie allerdings in Zusammenhang mit dem Verletzungsverbot verwendet hat.<sup>2</sup> Die Adaption der Formulierung wurde von den beiden Anwälte Warren und Brandeis dahingehend begründet, dass das Eindringen in den privaten Bereich dem Betroffenen mehr Schmerzen und Sorgen bereite, als es durch eine körperliche Verletzung möglich wäre.<sup>3</sup> Zukunftsblickend richtete sich ihre Tadelschrift dabei nicht bloss gegen die Verletzung eines persönlichen Rückzugortes, sie richtete sich ebenfalls gegen die unbefugte Verwertung privater Informationen.<sup>4</sup> «A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully, (...) What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself. It is not the intellectual product, but the domestic occurrence.»<sup>5</sup> Es dauerte dann aber noch fast 40 Jahre, bis 1928 das «right to be let alone» Eingang in die Rechtsprechung des US Supreme Court fand, dann aber gleich als «the most comprehensive of rights and the right most valued by civilized men».<sup>6</sup>

Schneller war das Schweizer Bundesgericht, welches bereits 1918 den Anspruch auf *Schutz der Privatsphäre* anerkannt hatte.<sup>7</sup> Dabei hat es festgehalten, dass es sich bei der Unverletzlichkeit der Privatsphäre um ein Rechtsgut handle, welches als Teil der Persönlichkeit vom Gesetz, konkret von Art. 28 ZGB, geschützt werde. Diese Bestimmung sichere nicht nur den Schutz der Persönlichkeit im Allgemeinen zu, vielmehr normiere sie auch das Recht auf Achtung der Privatsphäre,<sup>8</sup> indem sie dem einzelnen höchstpersönliche, absolute, unveräusserliche und unverjährbare Rechte

---

<sup>2</sup> COOLEY, S. 29.

<sup>3</sup> WARREN/BRANDEIS, S. 193 ff.

<sup>4</sup> AMELUNG, S. 52.

<sup>5</sup> WARREN/BRANDEIS, S. 193 ff.

<sup>6</sup> *Olmstead vs United States*, 277 U.S. 438, 478.

<sup>7</sup> «La vie en société exige que chacun puisse compter sur la discrétion d'autrui, sans avoir à craindre d'être épié dans son existence privée et de voir sa tranquillité troublée» (BGE 44 II 319 ff. (320), E. 1.

<sup>8</sup> BGE 44 II 319 ff. (320), E. 1.

verleihe.<sup>9</sup> Die Statuierung eines allgemeinen Grundsatzes und der Verzicht auf eine abschliessende Bestimmung des Begriffs der Persönlichkeit verliehen dem privatrechtlichen Persönlichkeitsschutz von Art. 28 ZGB eine «Vorbild- und Bezugsfunktion für den Grundrechtsschutz».<sup>10</sup> Die Anerkennung eines *verfassungsmässigen Persönlichkeitsschutzes* war zu dieser Zeit aber noch kein Thema. 1963 anerkannte das Bundesgericht die persönliche Freiheit als ungeschriebenes Grundrecht der Bundesverfassung,<sup>11</sup> und obwohl es den sachlichen Schutzbereich der persönlichen Freiheit anfangs sehr restriktiv festgelegt hatte und nur die Bewegungsfreiheit sowie die körperliche Freiheit darunter subsumierte,<sup>12</sup> fand eine allmähliche Ausdehnung des Schutzbereichs statt.<sup>13</sup> Die Ausweitung der persönlichen Freiheit zu einer allgemeinen Handlungsfreiheit, wie sie in Deutschland anerkannt war und ist,<sup>14</sup> verfolgte das Bundesgericht jedoch nicht.<sup>15</sup> Die persönliche Freiheit umfasse nicht jede noch so nebensächliche Wahl oder Betätigungsmöglichkeit des Menschen; der Schutzbereich des Grundrechts sei vernünftig auf die *elementaren Erscheinungen* der Persönlichkeitsentfaltung zu begrenzen.<sup>16</sup> Als eine derartige elementare Erscheinung der Persönlichkeitsentfaltung ordnete das Bundesgericht das Recht auf Privatsphäre erst 1976 dem Schutzbereich der persönlichen Freiheit zu.<sup>17</sup> Weitere elf Jahre danach erwog es in Anerkennung der zunehmenden Informatisierung der Datenbearbeitung, dass der sachliche Schutzbereich der persönlichen Freiheit auch punktuell den Schutz der *informationellen Privatheit* umfasse.<sup>18</sup>

---

<sup>9</sup> SCHWEIZER, SG-Komm BV, N 5 zu Art. 10 BV.

<sup>10</sup> SCHWEIZER, SG-Komm BV, N 5 zu Art. 10 BV.

<sup>11</sup> BGE 89 I 98 ff.

<sup>12</sup> BELSER, Datenschutzrecht, § 6 N 9.

<sup>13</sup> Siehe dazu statt vieler: BGE 97 I 842 ff. und BGE 99 Ia 504 ff.

<sup>14</sup> LABSCH, S. 51 ff.

<sup>15</sup> BGE 102 Ia 321 ff. (324 f.), E. 3a.

<sup>16</sup> Statt vieler: BGE 101 Ia 336 ff. (346 f.), E. 7a.

<sup>17</sup> BGE 102 Ia 516 ff. (522), E. 4.

<sup>18</sup> BGE 113 Ia 257 ff. (264 f.), E. 4c f.

## **2 Konzeption eines Rechts auf informationelle Selbstbestimmung**

Drei Jahre bevor das Bundesgericht überhaupt erst die persönliche Freiheit als ungeschriebenes Grundrecht anerkannte, wurde in Deutschland bereits der Grundstein für die informationelle Selbstbestimmung gelegt. In einer Abhandlung von EVERS ist zu lesen, dass die Selbstbestimmung über die persönlichen und privaten Angelegenheiten ein wesentlicher Bestandteil des Grundrechts auf Wahrung der Privatsphäre sei. Nur wenn eine solche eigene Sphäre, die fremden Augen und Ohren verschlossen bleibt, gegeben ist, könne der einzelne seiner Aufgabe zur eigenverantwortlichen Selbstbestimmung gerecht werden.<sup>19</sup>

Der Begriff der *informationellen Selbstbestimmung* erschien jedoch erst 1971 in einem vom deutschen Bundesministerium des Innern in Auftrag gegebenen Gutachten von Prof. Dr. Wilhelm Steinmüller und fünf weiteren Verfassern über die Grundfragen des Datenschutzes. Darin wurde im Hinblick auf eine künftige Datenschutzgesetzgebung der vom Datenschutz zu regelnde Gegenstandsbereich ausgearbeitet und das Konstrukt eines Rechts auf informationelle Selbstbestimmung ins Leben gerufen, wobei es als Selbstbestimmungsrecht des einzelnen, welche Informationen dieser unter welchen Umständen an wen weitergibt, definiert wurde.<sup>20</sup>

## **3 Übernahme und Entwicklung durch das deutsche Bundesverfassungsgericht**

Gut zwölf Jahre später hat das deutsche Bundesverfassungsgericht (nachfolgend: Bundesverfassungsgericht) 1983 im sog. «Volkszählungsurteil»<sup>21</sup> gestützt auf das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht den Begriff der informationellen Selbstbestimmung übernommen und dessen Bedeutung für die Allgemeinheit verbindlich festgelegt. Nach Meinung des Gerichts setze die *freie Entfaltung der Persönlichkeit* unter den modernen Bedingungen der

---

<sup>19</sup> EVERS, S. 39 f.

<sup>20</sup> STEINMÜLLER ET AL., S. 88.

<sup>21</sup> BVerfGE 65, 1.

## II Geschichtlicher Abriss bis zur Aufnahme in die BV von 1999

Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Recht auf informationelle Selbstbestimmung «gewährleiste insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen».<sup>22</sup> Dieses Verständnis der Schutzwirkung schiesst nach THIEL jedoch weit über den Schutz der Privatsphäre hinaus, welcher ebenfalls als Ausprägung des allgemeinen Persönlichkeitsrecht gilt,<sup>23</sup> indem es dem einzelnen ein Verfügungsrecht über die ihn betreffenden Daten einräumt und den Schutz bereits auf die Stufe der Persönlichkeits*gefährdung* vorverlagert.<sup>24</sup> Das Bundesverfassungsgericht geht nämlich bereits dann von einem Grundrechtseingriff aus, wenn gegenwärtig (noch) gar keine nachteiligen Folgen aus dem Umgang mit Informationen entstanden sind oder bevorstehen, solche Auswirkungen jedoch künftig als möglich erscheinen;<sup>25</sup> aufgrund der vielfältigen Nutzungsmöglichkeiten der elektronischen Datenverarbeitung gebe es ungeachtet des Verwendungskontextes kein belangloses Datum mehr.<sup>26</sup> Der zentrale Gewährleistungsgehalt des Rechts auf informationelle Selbstbestimmung liege dementsprechend auch primär in seiner *Abwehrfunktion*. Der Grundrechtsträger werde vor staatlicher Fremdbestimmung beim Umgang mit den ihn betreffenden Daten geschützt und es werde ihm das Recht zugestanden, sich gegen eine derartige Fremdbestimmung unter Berufung auf die grundrechtliche Gewährleistung zur Wehr zu setzen.<sup>27</sup>

Darüber hinaus sah das Bundesverfassungsgericht im Recht auf informationelle Selbstbestimmung auch einen Anspruch auf Freiheit von einem «Gefühl des Überwachtwerdens»,<sup>28</sup> sie werde in diesem Zusammenhang als Bedingung für eine *autonome Verhaltenssteuerung* verstanden.<sup>29</sup> Ziel des Grundrechts auf informationelle

---

<sup>22</sup> BVerfGE 65, 1 (46).

<sup>23</sup> THIEL, S. 223.

<sup>24</sup> THIEL, S. 223.

<sup>25</sup> BVerfGE 120, 378 (397).

<sup>26</sup> BVerfGE 120, 378 (397 ff.).

<sup>27</sup> THIEL, S. 224.

<sup>28</sup> THIEL, S. 224.

<sup>29</sup> DENNINGER, S. 111.

## II Geschichtlicher Abriss bis zur Aufnahme in die BV von 1999

Selbstbestimmung sei demnach die Erhaltung der Entscheidungsfreiheit,<sup>30</sup> welche eine elementare Grundbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens darstelle.<sup>31</sup> Nach seinem Schutzziel und nach den damit verbundenen Inhalten betrifft das Recht auf informationelle Selbstbestimmung somit «den Schutz gegen, den Einfluss auf und das eigene Wissen über den Umgang anderer mit den einen selbst betreffenden Informationen und Daten».<sup>32</sup>

Die Herleitung über die Realisierungsbedingungen der Selbstbestimmung und über die Entscheidungs- und Verhaltensfreiheit zeigt gemäss ALBERS, dass das Schutzziel und das Schutzkonzept auf die grundrechtliche Determination des Umgangs staatlicher Stellen mit Informationen und Daten gerichtet sind, die sich auf die Grundrechtsträger beziehen. Dies werde aber übergangslos in eine diesen eingeräumte Befugnis umgesetzt, über die Preisgabe und Verwendung persönlicher Daten selbst zu bestimmen. Aufgrund der fehlenden Begründungsschritte bleibe das systematische Verhältnis zur Entscheidungs- und Verhaltensfreiheit mehrdeutig. Das Recht auf informationelle Selbstbestimmung werde deshalb teilweise im Sinne eines Grundrechtsvoraussetzungsschutzes interpretiert. Man könne es aber auch als ganz eigenständige Gewährleistung begreifen.<sup>33</sup>

## 4 Adaption durch das Bundesgericht

1987 hat das Bundesgericht zum ersten Mal auf das Volkszählungsurteil und das darin entwickelte Recht auf informationelle Selbstbestimmung verwiesen.<sup>34</sup> Der Verweis fand im Zusammenhang mit der *Registrierung* personenbezogener Daten und dem daraus resultierenden *Einschränkungsgefühl* beim Betroffenen statt. Konkret ging es um den Anspruch auf Akteneinsicht ausserhalb eines hängigen Verfahrens eines von der Polizei angehaltenen Mannes an einem von Homosexuellen frequen-

---

<sup>30</sup> VOGELSANG, S. 53.

<sup>31</sup> Vgl. BVerfGE 65, 1 (46).

<sup>32</sup> ALBERS, Informationelle Selbstbestimmung, S. 175.

<sup>33</sup> ALBERS, Informationelle Selbstbestimmung, S. 176.

<sup>34</sup> BGE 113 Ia 1 ff. (6), E. 4b.

tierten Ort. Das Bundesgericht hielt fest, dass die Registrierung von Daten einen engen Bezug zum noch ungeschriebenen Grundrecht auf persönliche Freiheit aufweise: «Soweit der Beschwerdeführer aus dem Umstand, dass er an einem Ort kontrolliert worden ist, an dem sich angeblich häufig Homosexuelle aufhalten sollen, allenfalls mit dem Kreis von Homosexuellen in Verbindung gebracht werden sollte, kann der Registereintrag für ihn von nicht geringer Tragweite sein und ihn aus diesem Grunde allenfalls davon abhalten, sich völlig frei zu bewegen.»<sup>35</sup> Mit zunehmender Nutzbarkeit und Verwendungsmöglichkeit der besagten Daten wachse die Betroffenheit in den persönlichen Verhältnissen und von der Dauer der Aufrechterhaltung hänge das «Festschreiben» der betroffenen Person ab.<sup>36</sup> Übernommen wurde insbesondere die zentrale Idee, dass sich eine Person bereits durch das Wissen um die Existenz identifizierender Daten bei jemand anderem in ihrer persönlichen Freiheit beschränkt fühlen kann. Von einer Übernahme der Konstruktion eines Rechts auf informationelle Selbstbestimmung, im Sinne eines Selbstbestimmungsrechts bezüglich der Verwendung der eigenen Daten, kann zu diesem Zeitpunkt jedoch noch kaum gesprochen werden. Gleichwohl anerkennt das Bundesgericht, dass durch das blosse Vorhandensein von Personendaten, in Verbindung mit den technischen Möglichkeiten, das Gefährdungspotential für die persönliche Freiheit des einzelnen massiv gestiegen ist und dass bereits das Vorhandensein einer solchen Gefahr ausreicht, um ihn in seinem Handeln einzuschränken, auch wenn noch keine Verletzung stattgefunden hat.<sup>37</sup>

1994 hat die Zivilabteilung (!) des Bundesgerichts das informationelle Selbstbestimmungsrecht erstmals explizit erwähnt und das *Akteneinsichtsrecht* als Teil davon anerkannt.<sup>38</sup> Ausser der Bemerkung, dass dieses Konzept auch der Datenschutzgesetzgebung des Bundes zugrunde liegt, entbehrt das Urteil jedoch jeglicher Konkretisierung dieses Rechts, es nimmt auch keinen Bezug auf die Gründe und Umstände der Übernahme aus der deutschen Rechtsprechung oder die Unterschiede zwischen den beiden Rechtsordnungen. 1996 stellte das Bundesgericht ausdrücklich fest, dass

---

<sup>35</sup> BGE 113 Ia 1 ff. (6), E. 4b.

<sup>36</sup> BGE 113 Ia 1 ff. (10 f.), E. 4d.

<sup>37</sup> BGE 113 Ia 1 ff. (6), E. 4b.

<sup>38</sup> BGE 120 II 118 ff. (121), E. 3a.

das Recht auf informationelle Selbstbestimmung sowohl von der Lehre als auch von der Rechtsprechung anerkannt werde.<sup>39</sup>

## 5 «Eingang» in die neue Bundesverfassung

Mit der Revision der Bundesverfassung von 1999 wurde der verfassungsrechtliche Persönlichkeitsschutz aufgegliedert: Mehrere Aspekte der bisher ungeschriebenen Garantie auf persönliche Freiheit haben Eingang in *spezifische Grundrechtsbestimmungen* gefunden, darunter auch der Schutz der Privatsphäre.<sup>40</sup> Einige Aspekte, wie beispielsweise die körperliche und geistige Unversehrtheit, werden heute zwar explizit in der Verfassung erwähnt, bleiben jedoch als unselbständige Grundrechte unter der Marginalie «persönliche Freiheit» aufgeführt.

Der Begriff der «informationellen Selbstbestimmung» fand hingegen keinen Niederschlag in der neuen Verfassung. Zwar wurden die persönlichen Daten neu explizit dem Schutz der Privatsphäre nach Art. 13 BV unterstellt, gemäss Wortlaut von dessen Absatz 2 beschränkt sich dieser Anspruch jedoch auf den *missbräuchlichen Umgang* damit. Die Botschaft spricht von einem «Anspruch auf Datenschutz» als Teilaspekt des Rechts auf eine persönliche Geheimsphäre. Er bedeute, dass staatliche Organe Personendaten nur bearbeiten dürfen, wenn dies notwendig und verhältnismässig sei und die Bearbeitung zweckgebunden erfolge. Der definierte Missbrauchsschutz werde zudem durch Einsichts- und Berichtigungsrechte der betroffenen Person sichergestellt.<sup>41</sup> Allerdings ist den Materialien kein Hinweis zu entnehmen, wonach mit der Verfassungsrevision eine Beschränkung der bisher ungeschriebenen Schutzgüter im Bereich der persönlichen Freiheit einhergehen soll. Insofern kann davon ausgegangen werden, dass die vor der Revision vom Bundesgericht definierten Rechtsansprüche des einzelnen bezüglich die ihn betreffenden Daten (siehe nachfolgend) auch unter der neuen Verfassung weiterhin Geltung haben.

---

<sup>39</sup> BGE 122 I 153 ff. (162), E. 6b.

<sup>40</sup> Siehe BGE 127 I 6 ff. (11), E. 5a.

<sup>41</sup> Botschaft BV, S. 153.



RHINOW/SCHEFER sind der Ansicht, dass der Verfassungsgeber die Entwicklung eines ungeschriebenen Grundrechts auf informationelle Selbstbestimmung durchaus aufgenommen habe und dieses in der neuen Verfassung um die Garantien des Persönlichkeitsschutzes der EMRK ergänze, insbesondere um die von Art. 8 EMRK.<sup>42</sup> Die bewusste Übereinstimmung der beiden Schutzbereiche von Art. 13 BV und Art. 8 Abs. 1 EMRK habe nach BREITENMOSER denn auch zur Folge, dass eine implizite Anlehnung an die sehr umfangreiche Lehre und Rechtsprechung zu Art. 8 EMRK möglich sei.<sup>43</sup>

## 6 Résumé und Überleitung

Die Geschichte der informationellen Selbstbestimmung verläuft wie dargestellt keineswegs geradlinig. Obwohl das Bundesgericht den Anspruch auf Schutz der Privatsphäre bereits 1918 anerkannt hatte, dauerte es bis Mitte der 1970er-Jahre, bis es den Schutz der Privatsphäre als Teil des verfassungsrechtlichen Persönlichkeitsschutzes unter das bis dato noch ungeschriebene Grundrecht auf persönliche Freiheit subsumierte.<sup>44</sup> Mit der Verfassungsrevision von 1999 fand die persönliche Freiheit Eingang in das geschriebene Verfassungsrecht, wobei gewisse Teilgehalte als selbständige Grundrechte normiert wurden, darunter auch der Schutz der Privatsphäre. Der Begriff der informationellen Selbstbestimmung ist jedoch nicht in die Verfassung übernommen worden, wodurch die Fragen aufgeworfen werden, ob, und wenn ja, wie der Anspruch auf informationelle Selbstbestimmung Eingang in die Verfassung gefunden hat.

In den folgenden Kapiteln wird es deshalb darum gehen aufzuzeigen, wie Rechtsprechung und Lehre mit diesen Fragen umgegangen sind und wie der Gesetzgeber ein allenfalls bestehendes Grundrecht auf informationelle Selbstbestimmung umgesetzt hat.

---

<sup>42</sup> RHINOW/SCHEFER, RZ 1237.

<sup>43</sup> Vgl. BREITENMOSER, SG-Komm BV, N 2 f. zu Art. 13 BV.

<sup>44</sup> BGE 102 Ia 516 ff. (522), E. 4.

## III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

### 1 (Weitere) höchstrichterliche Auseinandersetzung

#### 1.1 Konkretisierungsschwierigkeiten

Die Einführung von Art. 13 Abs. 2 BV führte beim Bundesgericht zu Beginn zu keinerlei Änderung hinsichtlich der Anerkennung eines Rechts auf informationelle Selbstbestimmung. Im Gegenteil. Die zurückhaltende Formulierung des Art. 13 Abs. 2 BV wurde, soweit ersichtlich, in keinem Urteil thematisiert. Das Bundesgericht interpretierte die Bestimmung vielmehr kommentarlos *praeter verba legis* und unterstellte ihr, den Schutz des informationellen Selbstbestimmungsrechts als neues verselbständigtes Grundrecht.<sup>45</sup> In BGE 129 I 232 ff. führte es präzisierend aus, dass dem einzelnen gestützt auf Art. 13 Abs. 2 BV das Recht zukomme, selbst darüber zu bestimmen, ob und zu welchen Zweck Informationen über ihn bearbeitet werden.<sup>46</sup> Darüber hinaus hat das Bundesgericht den *Schutzbereich* dieser Bestimmung jedoch lediglich durch einige wenige Anwendungsbeispiele skizziert. So sind etwa die Erstellung eines DNA-Profiles und dessen Bearbeitung durch staatliche Behörden,<sup>47</sup> die gegen den Willen des Betroffenen veröffentlichte Fotografie<sup>48</sup> oder die 100-tägige Aufbewahrungsdauer von Videoaufzeichnungen durch die Polizei<sup>49</sup> unter Art. 13 Abs. 2 BV zu subsumieren.

Mit der Verfassungsrevision kamen jedoch auch *Abgrenzungsfragen* zum Schutzbereich anderer Grundrechte hinzu, welche vormals ebenfalls unter das ungeschriebene Grundrecht der persönlichen Freiheit gefallen sind. Laut Bundesgericht stelle Art. 10 Abs. 2 BV nach wie vor die verfassungsrechtliche Grundgarantie zum Schutz der Persönlichkeit dar, wovon neben dem Recht auf körperliche und geistige Unversehrtheit und auf Bewegungsfreiheit auch weiterhin all jene Freiheiten geschützt

---

<sup>45</sup> BGE 128 II 259 ff. (268), E. 3.2 f.; BGE 129 I 232 ff. (245), E. 4.3.1; BGE 133 I 77 ff. (85); E. 5.3.

<sup>46</sup> BGE 129 I 232 ff. (245), E. 4.3.1.

<sup>47</sup> BGE 128 II 259 ff. (268), E. 3.2.

<sup>48</sup> BGE 127 III 481 ff. (493), E. 3b.

<sup>49</sup> BGE 133 I 77 ff. (85), E. 5.3.

würden, die elementare Erscheinungen der Persönlichkeitsentfaltung verkörpern.<sup>50</sup> Demgegenüber schütze Art. 13 Abs. 2 BV den einzelnen vor Beeinträchtigungen, welche durch die staatliche Bearbeitung seiner persönlichen Daten entstehen.<sup>51</sup> Soweit die persönliche Integrität durch staatliches Datenbearbeiten gefährdet ist, kommt somit gemäss höchstrichterlicher Rechtsprechung der Schutz von Art. 13 Abs. 2 BV zum Tragen, wohingegen Art. 10 Abs. 2 BV als Auffanggrundrecht verstanden wird, sobald das einschlägige Grundrecht keinen genügenden Schutz mehr bietet. Diese klar scheinende Abgrenzung trägt jedoch insoweit, als dass das Bundesgericht bislang auf eine klare Umschreibung des Schutzbereichs von Art. 13 Abs. 2 BV verzichtet hat und somit im Zweifelsfall beide Grundrechte angerufen werden müssen.<sup>52</sup> Hinzu kommt, dass das Gericht in BGE 128 II 259 ff. den verfassungsrechtlichen Datenschutz als Teil des Rechts auf eine Privat- und persönliche Geheimsphäre nach Art. 13 Abs. 1 BV interpretiert hat.<sup>53</sup>

#### **1.2 Neuere Entscheide – Selbstbestimmung tritt in den Hintergrund**

Die neuere Rechtsprechung vermag die Konfusion nur weiter zu schüren, indem in den aktuellen Entscheiden vor allem der Schutz vor *missbräuchlicher Datenbearbeitung* hervorgehoben wird,<sup>54</sup> wohingegen dem Aspekt der Selbstbestimmung kaum mehr Beachtung geschenkt wird. So hat das Bundesgericht in BGE 138 I 331 ff. die Rechtmässigkeit einer Gesetzesänderung der *öffentlichen Sozialhilfe des Kantons Bern* gutgeheissen, welche vorsieht, dass die mit dem Vollzug des Gesetzes betrauten Personen von den Betroffenen zum Zeitpunkt der Einreichung des Gesuchs um Gewährung der Sozialhilfe eine Vollmacht zur Informationsbeschaffung bei diversesten Personen verlangen können.<sup>55</sup> Die Tatsache, dass der gesuchstellenden Person

---

<sup>50</sup> BGE 128 II 259 ff. (268), E. 3.2.

<sup>51</sup> BGE 129 I 232 ff. (245), E. 4.3.1.

<sup>52</sup> Immerhin hat das Bundesgericht ebenfalls festgehalten, dass ein generelles Recht, jederzeit zu wissen, wer was über einem weiss, in dieser allgemeinen Form als kaum praktikabel erachte (BGE 124 I 176 ff. (183), E. 6a).

<sup>53</sup> BGE 128 II 259 ff. (268), E. 3.2, wiederholt in BGE 138 I 331 ff. (337), E. 5.1.

<sup>54</sup> Um nur einige zu nennen: BGE 138 I 6 ff. (35), E. 7.3; BGE 136 II 508 ff. (522), E. 6.3.1, BGE 133 I 77 ff. (81), E. 3.2.

<sup>55</sup> BGE 138 I 331 ff.

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

keine andere Wahl bleibt, wenn ihr Gesuch weiter bearbeitet werden soll, und dass damit die Freiheit als wesentliche Voraussetzungen für eine rechtmässige Einwilligung fehlt, übergeht das Bundesgericht grosszügig. «Die alleinige Tatsache, dass eine Verweigerung der Vollmacht einen Nachteil für die betroffene Person nach sich zieht, (kann) die Gültigkeit der Zustimmung nicht beeinträchtigen. Dies wäre nur dann der Fall, wenn dieser Nachteil keinen Bezug zum Zweck der Bearbeitung hat oder diesem gegenüber unverhältnismässig ist.»<sup>56</sup> Der Hinweis des Bundesgerichts, dass die Betroffenen ja über einen verfassungsrechtlichen Anspruch auf Einsicht in ihre eigenen Akten hätten, womit ihnen die Möglichkeit bleibe, im konkreten Einzelfall eine verfassungswidrige bzw. gesetzeswidrige Anwendung der Vollmacht zu rügen,<sup>57</sup> vermag die Scheinheiligkeit und die fehlende Kontinuität der Rechtsprechung kaum aufzuheben.

Im *Google-Street-View-Entscheid*<sup>58</sup> hat sich das Bundesgericht weiter von der Konstruktion der informationellen Selbstbestimmung entfernt, indem es «angesichts der in der heutigen Gesellschaft faktisch bestehenden Einbindung von Personendaten in die soziale Realität» darauf verzichtete, eine vollständige Anonymisierung von Gesichtern und Autokennzeichen zu verlangen. Ein totaler Schutz vor Bildveröffentlichungen könne nicht gewährleistet werden. Ausserdem hätten die Bilder häufig nur eine geringe Persönlichkeitsrelevanz.<sup>59</sup> Das Bundesgericht begnügte sich deshalb in der Folge auch damit, dass durch verschiedene Massnahmen (Ankündigung der Kamerafahrten, Festlegung der Aufnahmehöhe, Widerspruchsmöglichkeit der Betroffenen etc.) die Wahrscheinlichkeit einer Persönlichkeitsverletzung verringert wird.<sup>60</sup> Da bezweifelt werden muss, dass alle Betroffenen von den angekündigten Kamerafahrten Kenntnis erhalten oder diesen aufgrund der Wohn- und/oder Arbeitssituation immer ausweichen könnten, ist es offensichtlich, dass damit viele Personen gegen ihren Willen gefilmt werden, was deutlich gegen eine informationelle Selbstbestimmung spricht.

---

<sup>56</sup> BGE 138 I 331 ff. (343 f.), E. 7.4.1.

<sup>57</sup> BGE 138 I 331 ff. (348), E. 7.4.3.2.

<sup>58</sup> BGE 138 II 346 ff.

<sup>59</sup> BGE 138 II 346 ff. (372), E. 10.6.6.

<sup>60</sup> BGE 138 II 346 ff. (376 ff.), E. 14.1 ff.

Interessanterweise kam das *Bundesverwaltungsgericht* ungefähr zum gleichen Zeitpunkt zum Schluss, dass jeder Person nach Art. 13 BV Anspruch auf Achtung ihrer Privatsphäre und Schutz vor Missbrauch ihrer persönlichen Daten habe. Dieser Anspruch bilde Teil der verfassungsmässigen Garantie der Privatsphäre und Kernbestandteil des Datenschutzgesetzes und räume jeder Person das Recht darauf ein, *selbst zu entscheiden, wann und wem sie persönliche Lebenssachverhalte, aber auch Gedanken, Empfindungen und Ähnliches preisgibt*. Dieses verfassungsmässige Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Abs. 1 EMRK) lasse grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem einzelnen die Herrschaft über seine personenbezogenen Daten zukommen und schütze ihn vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen.<sup>61</sup>

#### 1.3 **Fazit**

Trotz des Fehlens einer klaren und einheitlichen Rechtsprechung, kann davon ausgegangen werden, dass das Bundesgericht ein Grundrecht zum Schutz des einzelnen in Bezug auf seine Daten anerkennt. Ob es dabei von einem Grundrecht auf informationelle Selbstbestimmung oder bloss von einem Missbrauchsverbot ausgeht, kann angesichts der intransparenten oder gar inexistenten Begründungen nicht nachvollzogen werden. Immerhin scheint das Bundesverwaltungsgericht noch am Anspruch auf informationelle Selbstbestimmung festzuhalten.

## 2 **Bundesgesetzgeberische Auseinandersetzung**

Auch der Bundesgesetzgeber hat sich mit dem Grundrecht auf informationelle Selbstbestimmung auseinandergesetzt, jedoch ist diese Auseinandersetzung weder mit den bundesgerichtlichen Implementierungs- und Konkretisierungsbemühungen noch mit der verfassungsrechtlichen Verankerung kohärent. Dies dürfte daran liegen, dass der Bundesgesetzgeber bereits vor der Übernahme des Konstrukts der informationellen Selbstbestimmung Bedrohungen, welche wir heute darunter subsumieren

---

<sup>61</sup> Urteil des Bundesverwaltungsgerichts vom 10. April 2012 (A-4467/2011) in der Sache EDÖB gegen AXA Stiftung Berufliche Vorsorge Winterthur und EDI.

würden, mittels Normen abfederte, die nicht primär Datenbearbeitungen im Fokus hatten, und diese Normen heute noch ihre Geltung beanspruchen. Zu denken ist hier etwa an *Art. 28 ZGB*, welcher ganz grundsätzlich dem Schutz der Persönlichkeit gewidmet ist. Darüber hinaus ist es für den Gesetzgeber nicht einfach, sich mit einem Grundrecht konsistent durch die gesamten Bundesrechtsordnung auseinanderzusetzen, da den jeweiligen Rechtsgebieten unterschiedliche Maximen zugrunde liegen.

Da die Betrachtung aller sich mit dem Umgang mit Personendaten befassenden bundesgesetzgeberischen Normen den Rahmen des hier Darzulegenden sprengen würde, stehen im Folgenden vor allem die Bestimmungen des *DSG* als Grundsatzgesetz in Bezug auf den Umgang mit Daten im Fokus. Der Scope wird allerdings auf die *Art. 179 ff. StGB* ausgedehnt, da der Bundesgesetzgeber hier ebenfalls Bestimmungen erlassen hat, die sich in allgemeiner Weise<sup>62</sup> mit dem Umgang mit personenbezogenen Daten befassen.

## 2.1 Das DSG

### 2.1.1 Die Idee

Aufgrund des enormen Fortschritts im Bereich der Informationsverarbeitung und unter einem gewissen Druck der europäischen Entwicklungen im Bereich des Datenschutzes hat der eidgenössische Gesetzgeber die Notwendigkeit erkannt, rechtliche Leitplanken festzulegen, um die Entfaltung der Persönlichkeit des einzelnen ohne Beeinflussung durch unnötige und unerwünschte Informationstätigkeiten zu garantieren.<sup>63</sup> Am 19. Juni 1992 hat der Eidgenössische Gesetzgeber das DSG erlassen. Nach BELSER handelt es sich dabei um ein *Rahmengesetz*, das die allgemeinen Grundsätze der Datenbearbeitung sowie die Rechte des einzelnen festhält und institutionelle Aspekte regelt.<sup>64</sup> RUDIN spricht in diesem Zusammenhang auch von «formellem Datenschutzrecht», da das DSG selbst nicht die konkreten Datenbearbeitungen regelt, sondern «nur» die generellen Voraussetzungen und Anforderungen für

---

<sup>62</sup> Meint hier «nicht auf Daten aus einem bestimmten Fachbereich».

<sup>63</sup> Botschaft DSG, S. 417.

<sup>64</sup> BELSER, Datenschutzrecht, § 2 N 44.

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

das Datenbearbeiten.<sup>65</sup> Als *Querschnittsgesetz* findet das DSG sowohl auf Datenbearbeitungen durch Bundesorgane wie auch (natürliche oder juristische) Privatpersonen Anwendung. Dabei konkretisiert und ergänzt es einerseits den privatrechtlichen Persönlichkeitsschutz des ZBG, andererseits normiert es Grundsätze, welche sich aus der Bundesverfassung ergeben und die zu einem wesentlichen Teil vom Bundesgericht aus dem Recht auf persönliche Freiheit abgeleitet worden sind.<sup>66</sup> Dieser doppelte Regelungsbereich – Privatpersonen/Bundesorgane – ist nicht ganz unproblematisch, liegen ihm mit der Privatautonomie einerseits und dem Legalitätsprinzip andererseits grundverschiedene Konzepte zugrunde.

In der *Konzeption* des DSG geht der Gesetzgeber von einem weitreichenden Anspruch des einzelnen auf Autonomie im Bereich seiner persönlichen Daten aus. Dies ergibt sich einerseits daraus, dass er grundsätzlich anerkennt, dass der einzelne eine Art Herrschaft über seine Daten hatte, welche durch die modernen Datenverarbeitungsmethoden gefährdet ist: «Der einzelne (ist) vielfach nicht mehr in der Lage, auch nur annähernd abzusehen, wer wann wo welche Daten über ihn bearbeitet; er hat die Herrschaft über die Daten, die ihn angehen, weitgehend verloren.»<sup>67</sup> Damit werde der einzelne der Möglichkeit beraubt, selber zu bestimmen, wem er welche Mitteilungen machen will.<sup>68</sup> Andererseits ist es nach dem Willen des Gesetzgebers Aufgabe eines Datenschutzgesetzes, die Entscheidungsfreiheit der betroffenen Personen zu schützen<sup>69</sup> und zu verhindern, dass der einzelne zu einem rechtlosen Objekt von Informationstätigkeiten wird. Deshalb gewährt er ihm das Recht, Bild und Kenntnisse, die die Umwelt von ihm hat, bestimmen zu können:<sup>70</sup> «Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können.»<sup>71</sup>

---

<sup>65</sup> RUDIN, Verfassungswidrige Anwendbarkeit, S. 1 ff.

<sup>66</sup> BELSER, Datenschutzrecht, § 2 N 43.

<sup>67</sup> Botschaft DSG, S. 417.

<sup>68</sup> Botschaft DSG, S. 417.

<sup>69</sup> Botschaft DSG, S. 458.

<sup>70</sup> Botschaft DSG, S. 418.

<sup>71</sup> Botschaft DSG, S. 418.

#### 2.1.2 Der Gesetzestext

Der Gesetzestext selbst widerspiegelt auf den ersten Blick diese Ideen. So hält der erste Artikel fest: «Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.» Bei eingehender Betrachtung des DSG wird jedoch schnell klar, dass dem einzelnen sowohl bei Datenbearbeitungen durch Privatpersonen als auch bei Bearbeitungen durch Bundesorgane nur vordergründig ein Recht auf informationelle Selbstbestimmung zukommt.

##### 2.1.2.1 Bearbeiten von Personendaten durch Privatpersonen

Private dürfen Personendaten bearbeiten, d.h. erfassen, speichern, mit anderen Daten verknüpfen etc., solange sie dabei nicht die Persönlichkeit des Betroffenen widerrechtlich verletzen (Art. 12 Abs. 1 DSG). Persönlichkeitsverletzend ist ein Datenbearbeiten etwa dann, wenn die *wesentlichen Grundsätze* (u.a. Rechtmässigkeit, Treu und Glauben, Zweckbindung, Datensicherheit) nicht beachtet werden (Art. 12 Abs. 2 lit. a DSG) oder wenn Dritten besonders schützenswerte Personendaten oder Persönlichkeitsprofile bekannt gegeben werden (Art. 12 Abs. 2 lit. c DSG). Schliesslich liegt eine widerrechtliche Persönlichkeitsverletzung auch dann vor, wenn die Daten *gegen den ausdrücklichen Willen* der betroffenen Person bearbeitet werden (Art. 12 Abs. 2 lit. b DSG). Gerade durch die Möglichkeit, die Bearbeitung der eigenen Daten zu verbieten, soll das Selbstbestimmungsrecht der betroffenen Person über ihre Daten garantiert und geschützt werden.<sup>72</sup> Die hier statuierte Grenze wird allerdings so gleich wieder gelockert, äussert sich die Botschaft doch gegen eine zu strikte Handhabung derselben. Ein pauschales Verbot, die eigenen Daten zu bearbeiten, sei damit nicht gemeint, vielmehr gehe es um ein auf den Einzelfall gerichtetes Verbot gegenüber bestimmten Bearbeitern und bezogen auf bestimmte Bearbeitungsarten. Eine Persönlichkeitsverletzung liege zudem nur dann vor, wenn die betroffene Person die Datenbearbeitung ausdrücklich untersagt hat.<sup>73</sup> Hat ein Datenbearbeiter es lediglich unterlassen abzuklären, ob eine Person mit der Bearbeitung der sie betref-

---

<sup>72</sup> Botschaft DSG, S. 459.

<sup>73</sup> Vgl. ROSENTHAL, demgemäss diese enge Interpretation aufgrund des Wortlauts zumindest nicht zwingend wäre (ROSENTHAL, Handkommentar DSG, N 31 zu Art. 12).



fenden Daten einverstanden ist, so sei dies noch nicht als Persönlichkeitsverletzung im Sinne des DSG zu werten.<sup>74</sup>

Die Durchsetzung dieses *Widerspruchsrechts* setzt somit voraus, dass die betroffene Person Kenntnis von der Datenbearbeitung hat und –da es sich bei der vom Gesetz geforderten Willensäußerung um eine empfangsbedürftige Gestaltungserklärung handelt<sup>75</sup> – bedarf sie auch der Kenntnis des Datenbearbeiters. Diese Voraussetzungen scheinen trivial, sind es aber keineswegs. Aufgrund der unbeschränkten Verteilungsmöglichkeit von digitalen Daten ist es faktisch für den Betroffenen kaum mehr nachvollziehbar, wer seine Daten gerade wie verwendet (als Beispiel sei hier die Implementierung eines youtube-Videos auf einer anderen Homepage genannt). Dieser Umstand war dem Gesetzgeber auch durchaus bewusst, steht doch in der Botschaft zum DSG, dass der einzelne oft nicht imstande sei, Fehler und Missbräuche in der Informationsverarbeitung zu erkennen und die Verantwortlichen ausfindig zu machen.<sup>76</sup> Eine *Informationspflicht* sah er allerdings nur für das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen durch die Inhaber einer Datensammlung vor (Art. 14 DSG); beim Beschaffen von «gewöhnlichen» Personendaten besteht eine solche nicht.<sup>77</sup> Ferner besteht die Informationspflicht qua Gesetz auch nicht, wenn die betroffene Person bereits informiert wurde (Art. 14 Abs. 3 DSG) oder im Falle, dass die Daten bei Dritten beschafft werden, wenn die Datenspeicherung oder -bekanntgabe ausdrücklich im Gesetz vorgesehen ist oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (Art. 14 Abs. 4 DSG). Darüber hinaus fallen auch besonders schützenswerte Personendaten und Persönlichkeitsprofile, deren Erhebung nicht bezweckt wurde und welche quasi zufällig erfasst wurden, nicht darunter.<sup>78</sup> Die derart eingeschränkte Informationspflicht kann des Weiteren sogar wie die Auskunftspflicht nach Art. 9 DSG eingeschränkt werden, soweit ein Gesetz im formellen Sinn dies vorsieht, es wegen über-

---

<sup>74</sup> Botschaft DSG, S. 459.

<sup>75</sup> ROSENTHAL, Handkommentar DSG, N 29 zu Art. 12.

<sup>76</sup> Botschaft DSG, S. 417.

<sup>77</sup> Wer als Inhaber einer Datensammlung gilt resp. was unter Datensammlung zu verstehen ist, wird unterschiedlich definiert (vgl. hierzu ROSENTHAL/JÖHRI, Handkommentar DSG N 82 ff. zu Art. 3 lit. g DSG und BELSER, BaKomm DSG, N 31 f. zu Art. 3 lit. g DSG).

<sup>78</sup> RAMPINI/FUCHS, BaKomm DSG/BGÖ, N 8 zu Art. 14 DSG.

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

wiegender Interessen Dritter erforderlich ist oder wenn überwiegende Interessen des Inhabers der Datensammlung entgegen stehen und dieser die Personendaten nicht an Dritte bekannt gibt.

Mit den *Strafbestimmungen* des DSG sieht es kaum besser aus. Das Datenschutzgesetz kennt zwei Strafbestimmungen in Art. 34 und 35 DSG. Nach *Art. 34 DSG* können Private wegen Verletzung der *Auskunft-, Melde- und Mitwirkungspflichten* mit Busse bestraft werden. Dabei ist allerdings zu beachten, dass es sich bei der Verletzung dieser Pflichten gegenüber einer Privatperson um ein Antragsdelikt handelt und der Täter vorsätzlich gehandelt haben muss. Dies wiederum bedeutet, dass der Inhaber der Datensammlung, oder bei juristischen Personen deren Verantwortliche, genau wissen müssen, dass Daten betreffend eine bestimmte Person gesammelt worden sind, ansonsten der Vorsatz zu verneinen ist. Ist eine Datensammlung also schlecht organisiert, so dass sich deren Inhalt nicht mehr ermitteln lässt, ist der subjektive Tatbestand regelmässig nicht erfüllt.<sup>79</sup> *Art. 35 DSG* stellt demgegenüber die Verletzung der *beruflichen Schweigepflicht* unter Strafe. Wiederum handelt es sich dabei um ein Antragsdelikt und der Täter muss die Tat mit Vorsatz begangen haben. Da diese Bestimmung keine weitergehende Pflicht zur Beachtung der datenschutzrechtlichen Grundsätze statuiert, ist sie in Anbetracht von Art. 321 StGB (Verletzung des Berufsgeheimnisses) sogar obsolet.<sup>80</sup> Bemerkenswert ist, dass jeder andere Verstoß gegen die datenschutzrechtlichen Bestimmungen, sei es das unbefugte oder unverhältnismässige Erheben oder Sammeln von Personendaten, aber auch die Weigerung Daten zu löschen, vom DSG als nicht strafwürdig erachtet wird. De facto bedeutet dies einen Schlag ins Gesicht für die in der Botschaft noch hochgehaltene informationelle Selbstbestimmung, denn unrechtmässiges Verhalten wird nur in den wenigsten Fällen überhaupt strafrechtlich verfolgt und dies nur auf Antrag der betroffenen Person.

#### 2.1.2.2 *Bearbeiten von Personendaten durch Bundesorgane*

Möchten Bundesorgane Personendaten bearbeiten, so benötigen sie dazu eine *gesetzliche Grundlage*, die ihnen ebendiese Datenbearbeitung erlaubt (Art. 17 Abs. 1

---

<sup>79</sup> POLEDNA/CODONI, S. 278.

<sup>80</sup> Vgl. POLEDNA/CODONI, S. 279.

DSG). Besonders schützenswerte Personendaten oder Persönlichkeitsprofile dürfen sie nur dann bearbeiten, wenn dies ein Gesetz im formellen Sinn ausdrücklich vorsieht oder in *Ausnahmefällen*, wenn es für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist (sog. mittelbare Rechtsgrundlage), der Bundesrat es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind, oder die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 17 Abs. 2 DSG). Die Voraussetzung einer (formellen) Rechtsgrundlage entspricht dem verfassungsrechtlichen Grundsatz des Legalitätsprinzips und stellt zugleich die Rechtfertigung im Sinne von Art. 36 Abs. 1 BV dar, womit ihr grundsätzlich nichts entgegen gehalten werden kann. Es ist allerdings darauf hinzuweisen, dass die Bestimmungen, welche Datenbearbeitungen regeln, meist sehr offen und unbestimmt gehalten werden, womit dem Schutz der informationellen Selbstbestimmung nicht gedient ist, dieser gar ausgehöhlt werden kann.<sup>81</sup> Dies gilt auch in Bezug auf die Ausnahme, wonach die Datenbearbeitung für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist. Die Ausnahme, welche den Bundesrat ermächtigt, Datenbearbeitungen im Einzelfall zu bewilligen, weil die Rechte der betroffenen Person nicht gefährdet sind, ist als Notfallklausel zu werten, «um kurzfristig auftretenden Bedürfnissen Rechnung tragen zu können.»<sup>82</sup> Sie ist als Rechtsgrundlage nach Art. 17 Abs. 1 DSG für unvorhergesehene Datenbearbeitungen zu sehen. Als solche ist sie sehr offen formuliert und muss mit äusserster Zurückhaltung eingesetzt werden, um den Grundrechtsschutz, wie beschrieben, nicht auszuhöhlen. Bezüglich der Ausnahme der *Einwilligung* ist anzumerken, dass diese nur eingesetzt werden dürfte, wenn der einzelne auch eine echte Alternative hat und seine Entscheidung tatsächlich als freiwillig gewertet werden kann. Dies ist in der Praxis jedoch nicht immer der Fall, wie der Entscheid des Bundesgerichts zur öffentlichen Sozialhilfe des Kantons Bern augenfällig demonstriert.<sup>83</sup> Hinzu kommt, dass die Einwilligung in der Praxis auch gerne als Ersatz für eine fehlende Rechtsetzung eingesetzt wird, was ihrer hier zugewiesenen Funktion als Ausnahme jedoch klar wi-

---

<sup>81</sup> Zur Gefahr eines ausgehöhlten Grundrechtsschutzes siehe Kapitel IV, Ziffer 3; vgl. auch DRUEY, Strukturelle Schwächen, S. 146.

<sup>82</sup> Botschaft DSG, S. 468.

<sup>83</sup> BGE 138 I 331 ff.; diskutiert auf S. 13 f.

derspricht. Die von Art. 17 Abs. 2 DSG letztgenannte Ausnahme vom Erfordernis der Rechtsgrundlage, wonach die betroffene Person ihre Daten selbst *allgemein zugänglich* gemacht hat und eine Bearbeitung *nicht ausdrücklich untersagt* hat, hat sicherlich ihre Berechtigung, da bei einer Verwendung öffentlich gemachter Daten kein Grundrechtseingriff angenommen werden muss, womit es auch keiner Rechtfertigung bedarf. Dabei muss jedoch der Blickwinkel der betroffenen Person und deren mutmasslicher Wille beachtet werden: Wollte sie die Daten tatsächlich allen Personen zugänglich machen oder nur einem zwar grossen, aber immer noch begrenzten Personenkreis? Hierbei stellt sich u.a. die Frage, ob eine 350 Freunden bekannt gemachte Information auf Facebook noch als privat oder bereits als allgemein zugänglich zu qualifizieren ist. Ausserdem sind auch die «privacy policies» des jeweiligen Mediums zu beachten. Diese ändern beispielsweise bei Facebook derart häufig und für die User meist unbemerkt, dass von einem Tag auf den andern Daten, welche nur einem bestimmten Personenkreis zugänglich sein sollten, plötzlich allen Usern zugänglich sind. Davon können auch Daten von Personen betroffen sein, die selbst keinen Account beim jeweiligen Medium haben und die ihre Daten unter Umständen gar nicht, auch nicht einem begrenzten Userkreis, zugänglich machen wollen.<sup>84</sup> Immerhin bedarf es für die Inanspruchnahme dieser Ausnahmeregelung noch der Voraussetzung, dass die betroffene Person die Bearbeitung nicht ausdrücklich untersagt hat. Aufgrund des bereits zum *Widerspruchsrecht* Dargelegten, muss jedoch festgehalten werden, dass diese Ausnahmeregelung sehr weitläufig ist und nicht vorschnell angenommen werden darf.

Die *Informationspflicht* gilt auch für Bundesorgane. Im Gegensatz zur Informationspflicht von privaten Datenbearbeitern sind davon sämtliche Personendaten betroffen, auch solche, die bei Dritten beschafft werden (Art. 18a Abs. 1 DSG). An *Einschränkungsgründen* mangelt es jedoch auch in diesem Bereich nicht. So kann die Informationspflicht auf die Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen beschränkt werden, wenn sie die *Wettbewerbsfähigkeit* eines Bundesorgans beeinträchtigen würde (Art. 18a Abs. 5 DSG). Sie kann aber auch gänzlich entfallen, wenn die betroffene Person *bereits informiert* wurde, oder – sofern die Daten bei Dritten beschafft wurden – wenn die Speicherung und Bekanntgabe

---

<sup>84</sup> Vgl. zum Ganzen BAERISWYL, Kleingedrucktes, S. 56 ff.

der Daten ausdrücklich im Gesetz vorgesehen ist oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (Art. 18a Abs. 4 DSG). Die derart eingeschränkte Informationspflicht kann des Weiteren wie die Informationspflicht von privaten Datenbearbeitern nach Art. 9 Abs. 1 und 2 DSG eingeschränkt werden, soweit ein Gesetz im formellen Sinn dies vorsieht, es wegen überwiegender Interessen Dritter oder überwiegender öffentlicher Interessen erforderlich ist oder die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage stellt (Art. 18b Abs. 1 DSG).

#### 2.1.2.3 Der EDÖB

Der «Hüter des DSG» – der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) – ist nach Art. 29 Abs. 1 DSG im Rahmen von Datenbearbeitungen durch Private dazu verpflichtet, Sachverhalte näher abzuklären, wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl Personen zu verletzen (sog. *Systemfehler*), wenn Datensammlungen registriert werden müssen oder wenn eine Informationspflicht im Rahmen von Datenbearbeitungen im Ausland nach Art. 6 Abs. 3 DSG besteht. Dies bedeutet, dass wenn sich eine Person aufgrund einer Datenbearbeitung durch Private in ihrer Persönlichkeit verletzt sieht und es sich dabei nicht um einen Systemfehler handelt, der EDÖB nicht aktiv wird und der betroffenen Person nur die Klagemöglichkeit nach Art. 28 ZGB bleibt. Hinzu kommt, dass die ihm zur Verfügung stehenden Mittel *keinen Zwangscharakter* haben und lange Zeit in Anspruch nehmen, bis sie gegebenenfalls zum Erfolg führen. So kann der EDÖB aufgrund seiner Abklärungen empfehlen, das Bearbeiten zu ändern oder zu unterlassen (Art. 29 Abs. 3 DSG) und, wird einer solchen Empfehlung nicht gefolgt, kann er die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen, den er wiederum beim Bundesgericht anfechten kann (Art. 29 Abs. 4 DSG). Es kann nur mit dem politischen Willen resp. der Angst vor einem zu grossen Einfluss des EDÖB erklärt werden, dass der Gesetzgeber dem EDÖB nicht zumindest die Verfügungskompetenz einräumt.<sup>85</sup>

---

<sup>85</sup> ROSENTHAL, Handkommentar DSG, N 26 zu Art. 29 Abs. 3 DSG; vgl. auch HUBER, BaKomm DSG/BGÖ, N 44a zu Art. 29 DSG und BRUNNER, RZ 52, die eine Verfügungsmöglichkeit des EDÖB als wünschbar erachten.

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

In Bezug auf Datenbearbeitungen durch Bundesorgane kommt dem EDÖB hingegen eine umfangreiche Aufsichtskompetenz zu (Art. 27 DSG). Er überwacht nebst der Einhaltung des DSG auch die Einhaltung der übrigen Datenschutzvorschriften des Bundes durch die Bundesorgane (Art. 27 Abs. 1 DSG). Ergibt eine Abklärung, dass Datenschutzvorschriften verletzt werden, so empfiehlt er dem jeweiligen Bundesorgan, das Bearbeiten zu ändern oder zu unterlassen (Art. 27 Abs. 4 DSG). Wird eine solche Empfehlung nicht befolgt oder abgelehnt, so kann er die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5 DSG). Der EDÖB ist berechtigt, gegen diesen Entscheid Beschwerde zu führen (Art. 27 Abs. 6 DSG). Es kann diskutiert werden, ob der EDÖB nicht effizienter wäre, wenn er bei einer abgelehnten Empfehlung gleich verfügen könnte. Allerdings scheint der geltende Weg ein guter Kompromiss zu sein, wollten die Räte dem Beauftragten doch bei Erlass des DSG noch keinerlei Möglichkeit geben, verwaltungsinterne Entscheide gerichtlich überprüfen zu lassen.<sup>86</sup>

#### 2.1.3 Fazit

Die ursprüngliche Intention des Gesetzgebers beim Erlass des DSG – dem einzelnen die verlorene Herrschaft über seine Daten zurück zu geben – wurde im DSG nur teilweise adäquat umgesetzt. Gerade im Bereich der privaten Datenbearbeitung wird den Datenbearbeitern viel Spielraum gelassen. So ist eine nach DSG widerrechtliche Persönlichkeitsverletzung durch Private aufgrund der diversen Rechtfertigungsmöglichkeiten nur selten anzunehmen. Und auch dem Widerspruchsrecht nach Art. 12 Abs. 2 lit. b DSG fehlt aufgrund der nur eingeschränkten Informationspflicht der nötige Biss, zumal der Nachweis der erfolgten Widerspruchserklärung von den betroffenen Personen zu erbringen ist,<sup>87</sup> was ihr im Streitfalle einige Mühen bereiten dürfte.<sup>88</sup> Die sehr eingeschränkte Kontrollkompetenz des EDÖB verstärkt den Eindruck, dass der Gesetzgeber hier nur mit halbem Herzen dabei war.

In Bezug auf das Datenbearbeiten durch öffentliche Organe sieht die Beurteilung etwas anders aus: Die normierten Voraussetzungen sind gut nachvollziehbar und

---

<sup>86</sup> AmtlBull NR 1992, S. 389 f.; siehe auch HUBER, BaKomm DSG/BGÖ, N 16 zu Art. 27 DSG.

<sup>87</sup> RAMPINI, BaKomm DSG, N 11 zu Art. 12 DSG.

<sup>88</sup> ROSENTHAL, Handkommentar DSG, N 29 zu Art. 12.

können durchaus verfassungskonform umgesetzt werden. Die Informationspflicht ist breiter gefasst. Es gibt zwar auch hier viele Einschränkungsmöglichkeiten, doch nicht zuletzt in Anbetracht der ausgedehnten Aufsichtskompetenz des EDÖB kann hier von einer verfassungskonformen Umsetzung der informationellen Selbstbestimmung im Sinne der herrschenden Lehre (siehe Kapitel III, Ziffer 3) gesprochen werden.

## **2.2 Art. 179 ff. StGB - Strafbare Handlungen gegen den Geheim- oder Privatbereich**

### **2.2.1 Art. 179 StGB – Verletzung des Schriftgeheimnisses**

Als erstes widmet sich Art. 179 StGB der Verletzung des Schriftgeheimnisses, wobei auf Antrag mit Busse bestraft wird, wer ohne Berechtigung eine *verschlossene Schrift* oder Sendung öffnet, um von deren Inhalt Kenntnis zu nehmen, oder diesen nicht für ihn bestimmten Inhalt verbreitet oder ausnützt. Fraglich ist nun, ob auch die moderne Übermittlung solcher Schriften via *E-Mail* unter den Straftatbestand von Art. 179 StGB zu subsumieren ist.<sup>89</sup> In BGE 126 I 50 ff. hat das Bundesgericht entschieden, dass auch die Geheimsphäre eines E-Mail-Benutzers verfassungsrechtlich geschützt ist, womit der E-Mail-Verkehr über das Internet zum verfassungsmässigen Bereich des Fernmeldegeheimnisses gehört.<sup>90</sup> Interessant ist allerdings, dass nach Meinung von VON INS/WYDER E-Mails dennoch nicht unter das Schriftgeheimnis fallen. Dies wird zum einen damit begründet, dass E-Mails meist als Klartext versendet werden und somit nicht als «verschlossen» angesehen werden können. Aber auch wenn die nötigen Vorkehrungen getroffen würden, um von einer «verschlossenen Schrift» auszugehen, lehnen die Autoren die Subsumtion unter Art. 179 StGB aus prinzipiellen Überlegungen ab, da E-Mails aufgrund der ursprünglichen gesetzgeberischen Konzeption nicht als Sendung im Sinne von Art. 179 StGB verstanden werden können.<sup>91</sup> Diese Interpretation hätte zur Folge, dass das Öffnen der E-Mails sowie das Weiterverbreiten der daraus entnehmbaren Informationen nach StGB nicht

---

<sup>89</sup> Zur Frage, ob E-Mails Urkundenqualität haben können, siehe BGE 138 IV 209 ff., diskutiert von AENIS/MÜHLEMANN, S. 164 ff.

<sup>90</sup> VON INS/WYDER, BaKomm StGB, N 18 zu Art. 179 StGB.

<sup>91</sup> VON INS/WYDER, BaKomm StGB, N 20 ff. zu Art. 179 StGB.

strafbar wären.<sup>92</sup> VON INS/WYDER halten zwar richtig fest, dass die Bestimmung einen Teilaspekt des informationellen Persönlichkeitsschutzes darstelle und somit ein elementares Persönlichkeitsrecht schütze,<sup>93</sup> mit ihrer engen Interpretation wird jedoch schlicht der Zeitgeist verkannt, der bei der Auslegung einer Norm ebenfalls zu berücksichtigen ist.<sup>94</sup> Die heutige Kommunikation findet in unseren Breitengraden, aber auch über den Ozean hinaus, mehrheitlich mittels E-Mails statt. Es ist also mit ROSENTHAL und dem EDÖB einig zu gehen, dass die Norm immerhin so ausgelegt werden muss, dass es sich auch bei dem elektronischen Datenverkehr um eine verschlossene Sendung handelt, deren unberechtigtes Öffnen etc. nach Art. 179 StGB zu bestrafen ist.<sup>95</sup>

#### 2.2.2 Art. 179<sup>bis</sup> StGB – Abhören und Aufnehmen fremder Gespräche

Art. 179<sup>bis</sup> StGB schützt das Rechtsgut der Unbefangenheit der menschlichen Kommunikation in der Privatsphäre<sup>96</sup> und stellt auf Antrag das Abhören und Aufnehmen fremder Gespräche unter Strafe, wobei die Bestimmung ganze sechs Tatbestandsvarianten kennt.<sup>97</sup> Geschützt wird «jeder mündliche Gedanken- und Informationsaustausch», sofern der Täter nicht Gesprächsteilnehmer ist und das Gespräch in der Erwartung geführt wurde, dass ohne technische Mittel nicht mitgehört werden kann.<sup>98</sup> Das heisst, auch Selbstgespräche<sup>99</sup> oder offenbar sinnlose Äusserungen oder gar

---

<sup>92</sup> VON INS/WYDER, BaKomm StGB, N 26 zu Art. 179 StGB m.w.H.

<sup>93</sup> Vgl. VON INS/WYDER, BaKomm StGB, Kriminalstatistik, S. 920 und N 4 zu Art. 179 StGB.

<sup>94</sup> Nach KRAMER ist dem objektiv-teleologischen Argument im Gesamtzusammenhang der Interpretation der Vorrang (vor allen anderen Elementen) zuzurechnen (KRAMER, S. 152 f.); es bleibt allerdings zu beachten, dass diese Auslegungsmethode im Bereich des Strafrechts, wo ein strenges Analogieverbot gilt, mit einer gewissen Zurückhaltung auszuüben ist (vgl. KRAMER, S. 55).

<sup>95</sup> Wobei ROSENTHAL nur bei verschlüsseltem Datenverkehr von einer verschlossenen Sendung ausgeht, wohingegen der EDÖB auch bei einem nicht verschlüsselten Datenverkehr eine solche annehmen soll (ROSENTHAL, Projekt Internet, S. 24).

<sup>96</sup> VON INS/WYDER, BaKomm StGB, N 3 zu Art. 179<sup>bis</sup> StGB.

<sup>97</sup> Das Abhören mit einem Abhörgerät und Aufnehmen auf einem Tonträger von fremden nichtöffentlichen Gesprächen ohne Einwilligung (Abs. 1), das Auswerten und die Bekanntgabe von Tatsachen an Dritte, die durch das Abhören oder Aufnehmen bekannt geworden sind (Abs. 2) und das Aufbewahren oder Dritten Zugänglichmachen von Aufnahmen solcher Gespräche (Abs. 3).

<sup>98</sup> VON INS/WYDER, BaKomm StGB, N 8 ff. zu Art. 179<sup>bis</sup> StGB.

<sup>99</sup> VON INS/WYDER, BaKomm StGB, N 8 zu Art. 179<sup>bis</sup> StGB mit Verweis auf SCHERTH/JENNI.



der Gesang sind von der Bestimmung geschützt.<sup>100</sup> Relevant ist, dass diese Gespräche mit *technischen Hilfsmitteln* abgehört oder aufgezeichnet worden sind. Der Lauscher an der Wand bleibt demgemäss ebenso straflos wie jener, der ein ohne technische Hilfsmittel belauschtes Gespräch mitschreibt. Fraglich ist in diesem Zusammenhang die Strafbarkeit von sog. *Sekundäraufnahmen*, also die Aufnahme einer Aufnahme. Immerhin kann gesagt werden, dass im Falle einer rechtmässig erstellten Primäraufnahme das Erstellen einer Kopie davon nicht unter Art. 179<sup>bis</sup> StGB zu subsumieren ist, selbst wenn die Kopie ohne Einverständnis erfolgte.<sup>101</sup> Bei der Tatbestandsvariante des Auswertens oder der Weitergabe solcher illegal erhobenen Tatsachen ist zu beachten, dass der Täter bei nicht vorhandener Kenntnis der strafbaren Vortat mangels Vorsatz ebenfalls straflos bleibt. Die Tatbestandsvarianten des Aufbewahrens oder Zugänglichmachens beziehen sich wiederum auf die nach Abs. 1 illegal erhobenen Aufnahmen. Strafrechtlich verfolgt wird somit auch die Möglichkeit einer erneuten Verletzung der fremden Privat- oder Geheimsphäre.<sup>102</sup>

#### 2.2.3 Art. 179<sup>ter</sup> StGB – Unbefugtes Aufnehmen von Gesprächen

Nach Art. 179<sup>ter</sup> StGB wird auch jener Gesprächsteilnehmer auf Antrag bestraft, der ein nichtöffentliches Gespräch ohne Einwilligung der anderen Teilnehmenden auf einen Tonträger aufnimmt oder eine Aufnahme, von der er weiss oder annehmen muss, dass sie aus einem solchen Gespräch stammt, aufbewahrt, auswertet, einem Dritten zugänglich macht oder einem Dritten von dessen Inhalt Kenntnis gibt. Dieser *Insidertatbestand* soll die anderen Gesprächsteilnehmer davor schützen, dass ihre Äusserungen heimlich festgehalten werden und ihnen später durch Reproduktion zum Nachteil gereicht werden können.<sup>103</sup>

---

<sup>100</sup> VON INS/WYDER, BaKomm StGB, N 8 zu Art. 179<sup>bis</sup> StGB mit Verweis auf ERNI LORENZ, Die Verletzung der «Vertraulichkeit des Wortes» als Straftat im deutschen und schweizerischen Strafrecht, Diss. Zürich 1981, S. 108.

<sup>101</sup> VON INS/WYDER, BaKomm StGB, N 11 ff. zu Art. 179<sup>bis</sup> StGB.

<sup>102</sup> VON INS/WYDER, BaKomm StGB, N 30 zu Art. 179<sup>bis</sup> StGB.

<sup>103</sup> VON INS/WYDER, BaKomm StGB, N 2 zu Art. 179<sup>ter</sup> StGB.

#### 2.2.4 Art. 179<sup>quater</sup> StGB – Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte

Art. 179<sup>quater</sup> StGB stellt die Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte unter Strafe.<sup>104</sup> Im Gegensatz zu Art. 179 - Art. 179<sup>ter</sup> StGB geht es hier nicht um die Verletzung des Geheim- oder Privatbereichs durch das unbefugte Öffnen einer fremden Schrift oder Sendung oder durch das unbefugte Abhören und Aufnehmen von fremden nichtöffentlichen Gesprächen, sondern es geht um die *visuelle Bespitzelung* mittels technischer Geräte.<sup>105</sup> Das Bundesgericht hat dabei präzisiert, dass diese Bestimmung nicht nur vor der Aufnahme der Innenräume schützt, sondern auch den unmittelbar an das Wohnhaus angrenzenden Aussenbereich unter Schutz stellt.<sup>106</sup> Geschützt wird auch hier nicht ein spezifisches Datum, sondern «der Mensch soll in einer Atmosphäre der Zurückgezogenheit unbefangen und ungezwungen privaten, geheimen oder intimen Betätigungen nachgehen können, ohne gegen seinen Willen dabei beobachtet oder abgebildet zu werden».<sup>107</sup> RIKLIN spricht in diesem Zusammenhang vom Recht am eigenen Bild, weil ein Bild zeige, wer und wie ein Mensch ist.<sup>108</sup> Als Täter kommt allerdings nicht nur der heimliche Eindringling in Frage, sondern auch jener, der sich zwar mit Zustimmung des Betroffenen im geschützten Bereich befindet, jedoch ohne Kenntnis desselben Bildaufnahmen erstellt. Geschützt werden Tatsachen aus dem Privatbereich, also Ereignisse oder Zustände aus Gegenwart und Vergangenheit, die in irgendeiner Beziehung zum geschützten Privatbereich stehen. Dazu zählen neben Erscheinungsbild und Verhaltensweisen auch Bilder, Schriftstücke (nicht verschlossene) etc.<sup>109</sup> Innerhalb dieser geschützten Geheim- oder Privatsphäre sind nach VON INS/WYDER alle das *Eigenleben* einer Per-

---

<sup>104</sup> Auf Antrag bestraft wird, wer eine Tatsache aus dem Geheim- oder Privatbereich eines anderen oder eine nicht jedermann ohne weiteres zugängliche Tatsache aus dem Privatbereich eines anderen ohne dessen Einwilligung mit einem Aufnahmegerät beobachtet oder auf einen Bildträger aufnimmt (Abs. 1), aber auch wer eine Tatsache auswertet oder einem Dritten bekannt, von der er weiss oder annehmen muss, dass sie nach Abs. 1 illegal zu seiner Kenntnis gelangte (Abs. 2), genauso wie der, der durch eine Aufnahme, von der er selbiges weiss oder annehmen muss aufbewahrt oder eine Dritten zugänglich macht (Abs. 3).

<sup>105</sup> VON INS/WYDER, BaKomm StGB, N 2 zu Art. 179<sup>quater</sup> StGB.

<sup>106</sup> BGE 118 IV 41 ff. (49), E. 4e.

<sup>107</sup> VON INS/WYDER, BaKomm StGB, N 2 zu Art. 179<sup>ter</sup> StGB.

<sup>108</sup> RIKLIN, S. 535 f.

<sup>109</sup> VON INS/WYDER, BaKomm StGB, N 4 f. zu Art. 179<sup>quater</sup> StGB.

son betreffende Tatsachen geschützt, sogar solche, die keinen persönlichen Gehalt haben wie eine Liebesszene, Trauer oder unordentliche Kleidung.<sup>110</sup> Ziel war es, dem einzelnen die Möglichkeit zu geben und zu lassen, sich in seinem Privatbereich unbeobachtet, frei und sicher entfalten zu können.<sup>111</sup> Voyeurismus ohne Aufnahme-geräte, aber beispielsweise mit einem Feldstecher, ist straflos. Dagegen findet Art. 179<sup>quater</sup> StGB Anwendung bei Voyeurismus mit Aufnahmegerät, ohne dass das Gesehene aufgenommen wird.<sup>112</sup>

#### 2.2.5 «Relativierung» und Rechtfertigungsgründe

Die bis anhin dargestellten Strafbestimmungen dienen dem Schutz der Privatsphäre durch weitreichende Verbote im Umgang mit fremden personenbezogenen Daten, sofern der Betroffene im Einzelfall nicht die Zustimmung dazu gegeben hat. Allerdings handelt es sich bei allen um *Antragsdelikte*, was zur Folge hat, dass die Person von der Verletzung ihrer Rechte überhaupt erst Kenntnis erhalten muss. In Anbetracht der heute zur Verfügung stehenden subtilen Abhör- und Aufnahmemethoden (der Täter sitzt kaum mehr mit einem gut sichtbaren Teleobjektiv auf der Terrasse gegenüber), wird der Betroffene somit meist erst dann vom Verstoss erfahren, wenn die Daten an andere weiterverbreitet worden sind oder er damit konforntiert wird. Hier anzufügen bleibt, dass Art. 179<sup>quinquies</sup> (nicht strafbares Aufnehmen) und Art. 179<sup>octies</sup> (amtliche Überwachung, Straflosigkeit) StGB sowohl für Privatpersonen als auch für öffentliche Organe *Rechtfertigungsgründe* vorsehen, die das vorne beschriebene verbotene Verhalten legitimieren. Gerade beim staatlichen Rechtfertigungsgrund der *amtlichen Überwachung* ist darauf hinzuweisen, dass damit sehr weitgehend in die Privatsphäre der Betroffenen eingegriffen werden kann.

#### 2.2.6 Fazit

Die Strafbestimmungen Art. 179 ff. StGB dienen dem Schutz des Geheim- oder Privatbereichs, welcher, wie noch detailliert zu zeigen sein wird,<sup>113</sup> eine elementare Vo-

---

<sup>110</sup> VON INS/WYDER, BaKomm StGB, N 9 zu Art. 179<sup>quater</sup> StGB.

<sup>111</sup> VON INS/WYDER, BaKomm StGB, N 8 zu Art. 179<sup>quater</sup> StGB.

<sup>112</sup> VON INS/WYDER, BaKomm StGB, N 14 zu Art. 179<sup>quater</sup> StGB.

<sup>113</sup> Siehe Kapitel V – Schutzbedarfsanalyse.

raussetzung für die Entfaltung selbstbestimmter Individuen ist. Nach der Konzeption des StGB räumen sie den betroffenen Personen keine Rechte ein, sondern sie richten sich an die potentiellen Verletzter dieser Rechte, hier an Privatpersonen, die durch ihr Verhalten den sensiblen Bereich der Privatsphäre verletzen. Obwohl zu lesen ist, dass *Tatsachen* aus dem Privatbereich geschützt sind, geht es letztlich darum, dem einzelnen die Möglichkeit zu geben und zu lassen, sich in seinem Privatbereich unbeobachtet zu fühlen und sich damit frei und sicher entfalten zu können.

## 2.3 Fazit

Bereits diese überschaubare Darstellung der gesetzgeberischen Umsetzung der informationellen Selbstbestimmung zeigt den sich durch die gesamte Schweizer Geschichte dieses Rechts ziehenden, zwiespältigen Umgang damit. Gerade im Bereich der privaten Datenbearbeitung wird den Datenbearbeitern viel Spielraum belassen und eine Überprüfung durch den EDÖB kommt nur ausnahmsweise in Frage. Auch das Widerspruchsrecht nach Art. 12 DSG setzt hohe Hürden, nicht zuletzt in Bezug auf die Kenntnis der Datenbearbeitung sowie des Datenbearbeiters. Die dagegen angesetzte Informationspflicht gilt wiederum nur eingeschränkt, und es entsteht der Eindruck, der Gesetzgeber sei hier nur mit halbem Herzen bei der Sache gewesen. In Bezug auf das Datenbearbeiten durch öffentliche Organe entsteht eine andere Beurteilung, da die normierten Voraussetzungen durchaus verfassungskonform umgesetzt werden können und die Informationspflicht trotz diverser Einschränkungsmöglichkeiten breiter gefasst ist. Ein ähnliches Bild ergibt sich bei der Betrachtung des StGB: Ganz nach dem Charakter des Strafrechts werden hier klar umschriebene Handlungen bezüglich des privaten Umgangs mit Personendaten unter Strafe gestellt. Für Interpretationen besteht dadurch weniger Spielraum und der einzelne erlangt klare Ansprüche, welche er beim Staat anhängig machen kann. Dadurch wird der Eindruck erweckt, der Gesetzgeber wollte für diese von ihm ausgewählten Formen der Datenschutzverletzungen der informationellen Selbstbestimmung zur Durchsetzung verhelfen.

### 3 Auseinandersetzung in der Lehre

Die herrschende Lehre geht von einem *umfassenden verfassungsrechtlichen Persönlichkeitsschutz* aus, der gemeinsam von Art. 10 und 13 BV gewährleistet wird und der auch das Recht auf Selbstbestimmung bezüglich der eigenen Daten umfasst.<sup>114</sup> Eine klare Abgrenzung der Schutzbereiche beider Bestimmungen, oder vielmehr deren einzelner Absätze, hat sich jedoch als besonders schwieriges Unterfangen erwiesen, so dass die Meinungen, ob und wie diese Abgrenzung aussehen soll, stark divergieren.<sup>115</sup> Ein Teil der Lehre versteht Art. 10 BV als subsidiäre Garantie, welche dem einzelnen die persönliche Entfaltungsfreiheit in allen elementaren Lebensbereichen garantiert, während das Recht auf Privatsphäre nach Art. 13 BV als *lex specialis* gewährleistet, vom Staat in seinen privaten Angelegenheiten in Ruhe gelassen zu werden.<sup>116</sup> Dagegen führen Kritiker ins Feld, dass seit der Schaffung eines eigenständigen Rechts auf Privatsphäre zwei voneinander unabhängige Grundrechte nebeneinander stehen und nicht das eine dem anderen übergeordnet ist.<sup>117</sup> Einen ganzheitlicheren Ansatz vertritt demgegenüber BIAGGINI, der der Meinung ist, dass angesichts der «Hypertrophie» der Grundrechtsgarantien im Bereich des verfassungsrechtlichen Persönlichkeitsschutzes der Blick auf das Ganze zu bewahren sei und eine Verzettelung in Abgrenzungsfragen vermieden werden soll.<sup>118</sup> Gleichgültig, wie die Frage nach dem Verhältnis zwischen Art. 10 und 13 BV beantwortet wird, dürfte die einhellige Meinung bestehen, dass durch die Garantie eines Rechts auf Privatsphäre nach Art. 13 BV dem einzelnen jene Privatheit zugesichert werden soll, die er für die selbstbestimmte Entfaltung seiner Persönlichkeit braucht.<sup>119</sup> Und fast ebenso einhellig zeichnet sich demnach die Meinung ab, dass sich das Recht, selbst darüber zu bestimmen, ob, wem und wann jemand seine Gedanken, Gefühle, per-

---

<sup>114</sup> RHINOW/SCHEFER, RZ 1239; BIAGGINI, N 17 zu Art. 10 BV.

<sup>115</sup> M.w.Verw. BREITENMOSER, SG-Komm BV, N 5 zu Art. 13 BV.

<sup>116</sup> SCHWEIZER, SG-Komm BV, N 9 zu Art. 10 BV; KIENER/KÄLIN, S. 162.

<sup>117</sup> Vgl. GÄCHTER/EGLI, RZ 16 und 34; BREITENMOSER, SG-Komm BV, N 5 zu Art. 13 BV; zum Verhältnis allgemeines Persönlichkeitsrecht - Recht auf informationelle Selbstbestimmung in Deutschland siehe THIEL, S. 244.

<sup>118</sup> BIAGGINI, N 17 zu Art. 10 BV.

<sup>119</sup> Ausdrücklich RHINOW/SCHEFER, RZ 1241.

sönliche Sachverhalte oder Ideen offenbart, in Art. 13 Abs. 2 BV manifestiert.<sup>120</sup> Dass diese Interpretation der Bestimmung weit über deren Wortlaut, welcher bloss von einem Missbrauchsverbot spricht, hinausgeht, sei irrelevant, da der Verfassungstext zu eng gehalten sei.<sup>121</sup>

Um die Auseinandersetzung der herrschenden Lehre mit dem Grundrecht auf informationelle Selbstbestimmung besser abbilden zu können, werden deren Ansätze nachfolgend anhand der üblichen Struktur einer Grundrechtsanalyse dargestellt.

#### **3.1 Schutzzweck**

Hinter dem Grundrecht auf informationelle Selbstbestimmung verbirgt sich nach MÜLLER/SCHEFER die Idee, dass sich der einzelne nur dann selbstbestimmt und somit frei in der Gesellschaft bewegen kann, wenn er einigermaßen abzuschätzen vermag, wer welche persönlichen Informationen über ihn kennt,<sup>122</sup> was nur dann erreicht wird, wenn er grundsätzlich selbst bestimmt, wer welche Daten und Informationen zu seiner Person hat. Denn – wie noch vertieft zu zeigen sein wird – ermöglicht es u.a. gerade diese Einschätzung des Kenntnisstandes des Gegenübers, die diesem gegenüber zustehende Rolle einzunehmen. Kann der einzelne jedoch keine solche Abschätzung des Kenntnisstandes seines Gegenübers vornehmen, so wird er sich automatisch nicht mehr sicher in seiner für ihn zum Gegenüber bestehenden Rolle bewegen, sondern er wird versuchen, sich dem von ihm vermeintlich Erwarteten anzupassen.<sup>123</sup> Sein Entscheid, eine gewisse soziale Rolle zum Vis-à-vis einzunehmen, und sein darauf gerichtetes Verhalten erfolgen dann nicht mehr selbstbestimmt, sondern aufgrund eines vom einzelnen geglaubten erwünschten, gesellschaftlich akzeptierten Verhalten seiner Person.

---

<sup>120</sup> RHINOW/SCHEFER, RZ 1376; MÜLLER/SCHEFER, S. 164; KIENER/KÄLIN, S. 158 (wobei auf S. 161 nunmehr die Rede vom Schutz vor missbräuchlicher Datenbearbeitung ist, auf S. 163 dann wieder die Erwähnung eines Anspruchs auf informationelle Selbstbestimmung).

<sup>121</sup> RHINOW/SCHEFER, RZ 1376; SCHWEIZER, SG-Komm BV, N 72 zu Art. 13 BV; BIAGGINI, N 13 zu Art. 13 BV; RUDIN, Erosion, S. 425; KIENER/KÄLIN, S. 158.

<sup>122</sup> MÜLLER/SCHEFER, S. 165.

<sup>123</sup> Zur Problematik eines angepassten Verhaltens siehe Kapitel V, Ziffer 5.1.

Der Schutzzweck des Grundrechts auf informationelle Selbstbestimmung ist insoweit nach der herrschenden Lehre in der *Gewährleistung der Entscheidungsfreiheit* bezüglich der eigenen Daten und Informationen zu sehen, als essentielle Voraussetzung für die Entwicklung selbstbestimmter Individuen.

## 3.2 Grundrechtsträger

Alle *natürlichen Personen* sind dem Schutz des Rechts auf informationelle Selbstbestimmung unterstellt. Auch *juristische Personen des Privatrechts* können Grundrechtsträger sein, soweit die sie betreffenden Daten ein Verletzungspotential für ihre Persönlichkeit aufweisen, wie beispielsweise die Kreditwürdigkeit oder die steuerliche Beurteilung.<sup>124</sup> Demgegenüber können sich *juristische Personen des öffentlichen Rechts* aufgrund ihrer hoheitlichen Gewalt nach SCHWEIZER nicht auf die Grundrechte berufen.<sup>125</sup> Eine andere Auffassung könnte jedoch vertreten werden, wenn solche Unternehmen im wirtschaftlichen Wettbewerb stehen, da hier ein ähnliches Verletzungspotential für die Persönlichkeit wie bei juristischen Personen des Privatrechts ausgemacht werden kann. Es ist allerdings zu bemerken, dass der Umgang mit Daten und Informationen öffentlicher Organe, worunter auch die juristischen Personen des öffentlichen Rechts zu zählen sind, in den Datenschutz- und Öffentlichkeitsgesetzen normiert ist und nur in deren Schranken Spielraum besteht. So haben beispielsweise die öffentlichen Organe des Kantons Basel-Stadt eine Interessenabwägung vorzunehmen, wenn eine Person Zugang zu Informationen der Verwaltung möchte, und überwiegende öffentliche Interessen dem entgegenstehen (§ 29 i.V.m. § 32 IDG). Eine solche Interessenabwägung darf jedoch nicht willkürlich erfolgen und einseitig Interessen favorisieren,<sup>126</sup> weshalb letztlich nicht von Selbstbestimmung in Bezug auf die eigenen Daten und Informationen gesprochen werden kann. Auch Bundesorgane, für die Art. 23 DSG vorsieht, dass, wenn sie privatrechtlich handeln, die Bestimmungen für das Bearbeiten von Personendaten durch private Personen gelten, sind eben nicht frei in der Entscheidung, wie sie mit den eigenen Informationen und Daten umgehen, sie haben einfach andere Grundsätze zu befolgen. Demzu-

---

<sup>124</sup> SCHWEIZER, SG-Komm BV, N 73 zu Art. 13 BV.

<sup>125</sup> BGE 125 I 173 ff. (175), E. 1b.

<sup>126</sup> WALDMEIER, Praxiskommentar IDG, N 51 zu § 32 IDG.

folge ist festzuhalten, dass öffentliche Organe, miteingeschlossen die juristischen Personen des öffentlichen Rechts, nicht Träger des Grundrechts auf informationelle Selbstbestimmung sind.

## **3.3 Sachlicher Schutzbereich**

### **3.3.1 Schutzobjekt**

Dass man sich bei der Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung eher auf einem juristischen Trampelpfad als auf einer geebneten Strasse befindet, zeigt sich besonders deutlich daran, welche Mühe es bereitet, in der Literatur und der Rechtsprechung klare Aussagen zum Schutzobjekt dieses Grundrechts zu finden. Finden sich sodann konkrete Äusserungen zum Thema, ist deren Unterschiedlichkeit, wie nachfolgend zu zeigen sein wird, kaum zu übertreffen.

BIAGGINI ist der Ansicht, dass die informationelle Selbstbestimmung alle Angaben schützt, «die einen hinreichend engen Bezug zu einer (natürlichen oder juristischen) Person aufweisen»,<sup>127</sup> also beispielsweise der vom Arzt schriftlich in der Behandlungsdokumentation des A festgehaltene Befund «HIV positiv» oder der an B adressierte Brief mit der Anschrift «Psychiatrische Klinik Sonnmatt». Auch KIENER/KÄLIN und GÄCHTER/WERDER sind der Auffassung, dass *alle personenbezogenen Daten* geschützt sind.<sup>128</sup> Dagegen berichtet der Regierungsrat des Kantons Basel-Stadt berichtet dem Grossen Rat zur schriftlichen Anfrage von Ernst Jost bezüglich Überwachungskameras im öffentlichen Raum, dass das Schutzobjekt des in § 11 Abs. 1 lit. j KV konkretisierten Schutzes personenbezogener Daten noch weitgehend unbestimmt sei. Die KV-Bestimmung nenne zwar die personenbezogenen Daten, deren Schutz gewährleistet sei, aber es sei heute unbestritten, dass es nicht um den Schutz der Daten als solche gehe, sondern um die Menschen dahinter, um den *Schutz der Persönlichkeit* der Personen, über welche Daten bearbeitet werden, um die informationelle Selbstbestimmung.<sup>129</sup> Diese Auffassung würde auch der ur-

---

<sup>127</sup> BIAGGINI, N 12 zu Art. 13 BV.

<sup>128</sup> KIENER/KÄLIN, S. 158; GÄCHTER/WERDER, S. 91.

<sup>129</sup> Regierungsratsbeschluss, S. 2.



### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

sprünglichen Idee der informationellen Selbstbestimmung entsprechen, wurde doch schon im Gutachten von STEINMÜLLER ET AL. herausgearbeitet, dass es um ein Selbstbestimmungsrecht des einzelnen gehe, welche Informationen dieser unter welchen Umständen an wen weitergibt,<sup>130</sup> wobei gemäss VOGELSANG das entscheidende Kriterium das Bestimmungsrecht über die sich selbst betreffenden Informationen ist.<sup>131</sup> In diesem Sinne argumentiert auch GARSTKA, demgemäss die informationelle Selbstbestimmung dann weitest gehend verwirklicht ist, wenn die Entscheidung zur Offenbarung von Daten und der Bestimmung, wie sie verarbeitet werden sollen, vom der betroffenen Person selbst stamme.<sup>132</sup> Es wird also nicht das einzelne Datum vom Schutz der informationellen Selbstbestimmung erfasst, sondern die *Entscheidungsfreiheit* des einzelnen in Bezug auf die Verwendung seiner Daten. Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist auch nach RUDOLF am Schutzgegenstand der Selbstbestimmung des einzelnen über seine persönlichen Daten orientiert. Geschützt sei die Sicherung der Entscheidungsbefugnis des einzelnen gegenüber dem Umgang anderer mit seinen Daten. Das Recht auf informationelle Selbstbestimmung sei eine Ausformung des Schutzes der Vertraulichkeit im privaten Raum und des Rechts an der Darstellung der eigenen Person nach aussen. Es handle sich dabei um die Selbstverfügung über personenbezogene Daten, also um eine *selbstbestimmte Verhaltensentscheidung*.<sup>133</sup> Auch nach BRÜCKNER sind nicht die intimen und privaten Informationen als solche geschützt, «sondern die Selbstbestimmung der Person im Umgang mit dieser Information».<sup>134</sup> Dieser Auffassung ist zu folgen, da jede Person die Schutzwürdigkeit der auf sie referenzierenden Daten und Informationen individuell und nach Rolle und Beziehung differenziert beurteilt.

---

<sup>130</sup> STEINMÜLLER ET AL., S. 88.

<sup>131</sup> VOGELSANG, S. 24.

<sup>132</sup> GARSTKA, S. 169.

<sup>133</sup> RUDOLF, HGR, N 24 zu § 90. In N 30 zu § 90 ist dann jedoch zu lesen, dass Personendaten das Schutzobjekt darstellen.

<sup>134</sup> BRÜCKNER, RZ 487; ferner ist hier auch auf Literatur aus dem Bereich des Rechts am eigenen Bild zu verweisen, welches zweifellos ein Personendatum darstellt. So ist nach PREISWERK unter dem Recht am eigenen Bild die «alleinige Macht, das Abbild der eigenen Person zu veröffentlichen und allen anderen, nicht aus besonderem Grunde Befugten, die Publikation untersagen zu dürfen» zu verstehen (PREISWERK, S. 40) und KEYSSNER ist der Ansicht, dass jedweder seines Bildes Herr ist, «ohne seine Genehmigung darf er nicht durch Abbildung veranschaulicht oder durch Illustration berühmt gemacht werden». (KEYSSNER, S. 31 f.).

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

Dies an einem Beispiel verdeutlicht: Während die eine Person keinem Menschen von ihrer Diagnose «HIV positiv» erzählt, weil sie diese Information als besonders schutzwürdig erachtet, geht eine andere Person sehr offen damit um, misst dieser Information keine besondere Bedeutung zu. Bei der ersten Person wäre das Datum somit vom grundrechtlichen Schutzbereich erfasst, bei der zweiten Person nicht. Um einen Vergleich zu ziehen: Die Eigentumsgarantie nach Art. 26 BV schützt auch nicht die Sache (den Stuhl, die Tasche, das Haus etc.) an und für sich,<sup>135</sup> sondern die Rechtsposition des Eigentümers, im Rahmen der Rechtsordnung über sein Eigentum zu «verfügen».

Es kann sich beim Schutzobjekt also weder um das einzelne Datum handeln, noch kann es darum gehen, ob dieses aus der Privat- oder Intimsphäre stammt, da auch diese Beurteilung individuell ausfällt. Schutzobjekt kann einzig die Entscheidungsfreiheit der einzelnen Person sein, die es ihr gestattet, persönlichen Daten und Informationen je nach persönlichem Empfinden bekannt zu geben oder eben auch nicht. Dies bedeutet nicht, dass Daten an und für sich nicht schützenswert sein können und die Datenschutzgesetze, welche Regeln für den Umgang mit ihnen festlegen, ins Leere laufen würden. Daten sind jedoch nicht aufgrund ihrer *Art* als Daten schützenswert, sondern aufgrund ihres Potentials für Persönlichkeitsverletzungen, wenn sie ohne das Einverständnis ihres «Eigentümers» verwendet werden. Erneut illustriert am Beispiel der Eigentumsgarantie: Die von der Rechtsordnung festgelegten Regeln über den Umgang mit Eigentum laufen nicht ins Leere, nur weil die Sache selbst nicht das Schutzobjekt der grundrechtlichen Garantie ist. Die von der Rechtsordnung geschaffenen Regeln und Vermutungen dienen schlicht der Vereinfachung des täglichen Lebens in der Gesellschaft. So ist die in den Datenschutzgesetzen vorgenommene Einstufung der Gesundheitsdaten als besonders schützenswerte Personendaten eine aufgrund von Risikoüberlegungen getroffene Kategorisierung, da von ihnen eine grössere Gefahr für die Verletzung der Persönlichkeit ausgeht. Dies ist aber, wie das «HIV-positiv»-Beispiel weiter vorne zeigt, nicht zwingend, wenn die betroffene Person das Datum selber als nicht persönlichkeitsgefährdend einstuft. Es kann aber auch sein, dass ein von der Rechtsordnung als harmlos ein-

---

<sup>135</sup> Sonst gäbe es keine herrenlosen Sachen, die in niemandes Eigentum stehen, über die eben niemand das Verfügungsrecht inne hat.

gestuftes Datum wie die Adresse je nach Verwendungskontext (so beispielsweise im Bereich von Kindsentführungen) höchst sensibel ist und des erhöhten Schutzes bedarf, obwohl es vom Gesetz her so nicht vorgesehen ist (siehe Kapitel V, Ziffer 8).

#### 3.3.2 Schutzzumfang

Der vorne beschriebene Schutzzweck – die Gewährleistung der Freiheit zum selbstbestimmten Handeln in Bezug auf die eigenen Informationen und Daten und damit letztlich zur Selbstbestimmung an und für sich<sup>136</sup> – kann nur dann erreicht werden, wenn sich der Schutz des Grundrechts auf *sämtliches Datenbearbeiten* bezieht, ungeachtet des jeweiligen Verfahrens zur Datenverarbeitung.<sup>137</sup> Konkret sind damit die Erhebung, Aufbewahrung, Bearbeitung, Veränderung, Bekanntgabe,<sup>138</sup> aber auch die Löschung von Personendaten erfasst. Der Schutzbereich ist damit tangiert, sobald die Daten einer Person ohne deren Einverständnis bearbeitet werden,<sup>139</sup> ungeachtet davon, ob die Bearbeitung selbst zu einer Persönlichkeitsverletzung führt oder nicht.<sup>140</sup>

Unterschiedlich gestalten sich die Meinungen jedoch bezüglich des *Datenbearbeiters*. Fraglich ist insbesondere, ob nur Datenbearbeitungen durch staatliche Organe (kantonale wie Bundesorgane) unter den Schutzbereich fallen oder auch Datenbearbeitung durch Private davon erfasst sein sollen. Insbesondere RHINOW/SCHEFER vertreten die Ansicht, dass die Datenbearbeitung von einer Privatperson zu deren persönlichem Gebrauch nicht den Schutzbereich tangiert, soweit die Daten nicht an Dritte weitergegeben werden.<sup>141</sup> In Konsequenz der dargelegten Zielrichtung des Grundrechts auf informationelle Selbstbestimmung und in Anbetracht der Tatsache, dass auch privates Datenbearbeiten zu massiven Persönlichkeitsverletzungen führen kann, ist nach SCHWEIZER jedoch davon auszugehen, dass das informationelle Selbstbestimmungsrecht den einzelnen nicht nur bei staatlicher Bearbeitung seiner

---

<sup>136</sup> Zum Schutzzweck siehe Kapitel 5.

<sup>137</sup> Vgl. SCHWEIZER, SG-Komm BV, N 74 zu Art. 13 BV.

<sup>138</sup> SCHWEIZER, SG-Komm BV, N 74 zu Art. 13 BV.

<sup>139</sup> BELSER, Datenschutzrecht, § 6 N 88.

<sup>140</sup> Zur Auslegung von «Bearbeiten» siehe Kapitel VI, Ziffer 4.1.3.

<sup>141</sup> RHINOW/SCHEFER, RZ 1378.

### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

Daten schützt, sondern nach Art. 35 BV auch eine Schutzpflicht bezüglich privaten Datenbearbeitern beinhaltet.<sup>142</sup> Nimmt eine private Person eine staatliche Aufgabe wahr, so ist diese sogar unmittelbar an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen (Art. 35 Abs. 2 BV). Nimmt der Private keine staatliche Aufgabe wahr, ist er dennoch indirekt an die Grundrechte gebunden (Art. 35 Abs. 1 BV). Die aus dem Grundrecht fliessenden allgemeinen Grundsätze der Datenbearbeitung gelten dementsprechend nach SCHWEIZER gleichermassen für Datenbearbeitungen von Privaten wie auch von öffentlichen Organen.<sup>143</sup> Letztlich hängen die unterschiedlichen Meinungen mit der jeweiligen Haltung zur Wirkung der Grundrechte zwischen Privaten ganz allgemein zusammen, worauf unter Kapitel VI, Ziffer 2 vertieft eingegangen wird. Aufgrund des noch zu diskutierenden Schutzbedarfs vertritt die Autorin jedoch dezidiert die Auffassung, dass das Grundrecht auf informationelle Selbstbestimmung auch zwischen Privaten Geltung haben muss, wobei dann vor allem der Gesetzgeber gefragt ist, Regeln zu definieren, damit der Umgang mit Daten und Informationen alltagstauglich ist und beispielsweise einfaches Geschwätz oder das Duplizieren eines Familienfotos für die eigene Pinnwand nicht rechtsrelevant wird.<sup>144</sup>

Der Schutz der informationellen Selbstbestimmung lässt sich aufgrund der besonderen Eigenschaften der behandelten Materie Information/Daten offenbar nicht alleine durch dessen verfassungsrechtliche Verankerung gewährleisten. Deshalb umfasst dieses Grundrecht gewissen Autoren zufolge nicht nur die Gewährleistung des Rechts an sich, sondern darüber hinaus auch noch *konkrete Ansprüche* (Instrumente), welche die Durchsetzung des Grundrechts sichern sollen. Diese Ansprüche gehören gemäss SCHWEIZER zum Schutzzumfang,<sup>145</sup> weshalb sie an dieser Stelle behandelt werden. Sie könnten aber ebenso gut in einer eigenen Rubrik «Schutzgehalte» thematisiert werden.

Der einzelne vermag sein Recht, selbstbestimmt über seine Daten zu entscheiden, nur dann wahrnehmen, wenn er auch in Kenntnis davon ist, dass und welche Daten

---

<sup>142</sup> SCHWEIZER, SG-Komm BV, N 84 zu Art. 13 BV.

<sup>143</sup> SCHWEIZER, SG-Komm BV, N 84 zu Art. 13 BV.

<sup>144</sup> Zur indirekten Horizontalwirkung siehe Kapitel VI, Ziffer 2.2.

<sup>145</sup> SCHWEIZER, SG-Komm BV 2008, N 45 zu Art. 13 BV.

über ihn bearbeitet werden. Demgemäss ist nach SCHWEIZER das *Auskunftsrecht* ein zentraler Bestandteil des Rechts auf informationelle Selbstbestimmung.<sup>146</sup> Das Auskunfts- und Einsichtsrecht bezieht sich dabei nicht nur auf die Daten, die ursprünglich erhoben wurden, sondern auch auf jene Daten, welche durch das Bearbeiten der ursprünglichen Daten entstanden sind.<sup>147</sup> Darüber hinaus gehört nach BIAGGINI auch das Recht auf *Berichtigung* falscher bzw. auf *Löschung* ungeeigneter oder nicht mehr benötigter oder auf widerrechtliche Weise besorgter Daten zum Schutzzumfang, damit der Anspruch auf informationelle Selbstbestimmung bei Feststellen von Unrichtigkeiten nicht ins Leere läuft.<sup>148</sup> Diese Ansprüche ergeben sich zwar nicht direkt aus dem Wortlaut der Verfassungsbestimmung. Sie waren jedoch bereits vor der Revision durch das Bundesgericht anerkannt, und da den Materialien kein Hinweis zu entnehmen ist, dass der Schutzbereich durch die Verankerung in einem eigenen Artikel hätte eingeschränkt werden sollen, haben sie wohl auch weiterhin Bestand.<sup>149</sup>

#### **3.4 Kerngehalt**

Bei den Kerngehalten handelt es sich «um jene Aspekte menschlicher Existenz, die für den einzelnen von derart zentraler Bedeutung sind, dass ihm unter keinen Umständen zugemutet werden darf, sie aufzugeben».<sup>150</sup>

Soweit ersichtlich hat sich die herrschende Lehre wie auch die Rechtsprechung bislang nur sehr vage zu einer Umschreibung des Kerngehalts der informationellen Selbstbestimmung hinreissen lassen. In Anbetracht der weitreichenden Möglichkeiten, im Rahmen des *BÜPF* in den Schutzbereich des Grundrechts eingreifen zu können (Abhörung von Telefongesprächen, Überwachung des Mailverkehrs etc.), erscheint es denn auch äusserst schwierig, einen solchen zu umschreiben und daran festzuhalten. Nach SCHEFER betrifft die Frage nach der Geltung und dem Gehalt grundrechtlicher Kerngehalte allerdings das Fundament der Rechtsordnung

---

<sup>146</sup> SCHWEIZER, SG-Komm BV, N 85 zu Art. 13 BV.

<sup>147</sup> BELSER, Datenschutzrecht, § 6 N 99.

<sup>148</sup> BIAGGINI, N 14 zu Art. 13 BV.

<sup>149</sup> SCHWEIZER, SG-Komm BV 2008, N 37 zu Art. 13 BV.

<sup>150</sup> SCHEFER, Kerngehalte, S. 5.

schlechthin,<sup>151</sup> insoweit hier doch zumindest die Mühe eines Versuchs gemacht werden muss, einen Kerngehalt auch für das Grundrecht auf informationelle Selbstbestimmung zu definieren.

Mangels äquivalenter Schweizer Gerichtsurteile muss im Folgenden auf ein Urteil des Bundesverfassungsgerichts zurückgegriffen werden, um eine Annäherung an den Kerngehalt von Art. 13 Abs. 2 BV zu ermöglichen: 1989 hatte das Bundesverfassungsgericht im sog. Tagebuch-Beschluss einen Fall zu beurteilen, in dem ein Mann wegen Mordes an einer Frau zu einer lebenslangen Freiheitsstrafe verurteilt wurde.<sup>152</sup> Die Beweisführung des Urteils beruhte im Wesentlichen auf persönlichen Aufzeichnungen des Täters, in denen er sich auf Anraten seines Psychologen in der Art eines Selbstgespräches mit seinen psychischen Problemen auseinandersetzte. In seinen «Tagebüchern» legte der Täter u.a. dar, was ihn daran hinderte, Beziehungen zu Frauen einzugehen, wie es sich mit seiner aggressive Haltung dem anderen Geschlecht gegenüber verhielt, aber auch dass er Mitleid zu seinen potentiellen Opfer verspürte. Das Bundesverfassungsgericht hatte die Frage zu beurteilen, ob die Verwendung dieser intimen Aufzeichnungen im Strafverfahren den Kerngehalt des Persönlichkeitsrechts nach Art. 2 Abs. 1 GG verletze. Vier Richter teilten die Meinung, dass der Kerngehalt nicht berührt sei und die Verwendung der «Tagebücher» als Beweismittel somit als zulässig erachtet werden müsse. Die andere Hälfte der insgesamt acht Richter war jedoch der Auffassung, dass die fraglichen Aufzeichnungen von derart intimen Charakter seien, dass sie vor jedem Zugriff durch die Behörden geschützt werden müssen und eine Verwertung als Beweis die Persönlichkeit des Betroffenen im Kern verletze: «Die hier in Rede stehenden tagebuchähnlichen Aufzeichnungen haben ausschliesslich höchstpersönlichen Charakter. Sie enthalten eine offene, von *keiner Rücksichtnahme sich selbst gegenüber* beeinflusste Wiedergabe bestimmter Gemütszustände sowie Reflexionen über die eigene Persönlichkeitsstruktur, die der Beschwerdeführer durch eine schonungslose Darstellung seiner Gefühlswelt besser ergründen wollte, um auf diese Weise über zentrale ihn quälende Probleme mit sich ins Reine zu kommen. Diese Auseinandersetzung mit dem eigenen Ich, die nur so, wie geschehen, geführt wurde und geführt werden konnte, weil

---

<sup>151</sup> SCHEFER, Kerngehalte, S. 5.

<sup>152</sup> BVerfGE 80, 367.

sie in der Einsamkeit der Selbstgesprächs, also geschützt vor fremden Augen und Ohren stattfand, und auch in diesem Bereich verbleiben sollte, verlor ihren höchstpersönlichen Charakter nicht deshalb, weil sie dem Papier anvertraut wurde. So gewiss es ist, dass die Gedanken frei sind – und deshalb frei bleiben müssen vor staatlichem Zwang und Zugriff, wenn nicht der Mensch im Kernbereich seiner Persönlichkeit getroffen werden soll –, so gewiss muss gleicher Schutz für das schriftlich mit sich selbst geführte Gespräch gelten, bei dem das andere Ich durch die Niederschrift zum Sprechen gebracht und damit als Gegenüber besser verstanden wird.»<sup>153</sup>

Unter welchen Voraussetzungen der für einen absoluten Schutz erforderliche *höchst intime Charakter* zu bejahen ist, kann nicht in allgemeingültiger Art und Weise umschrieben werden. Jedoch ist festzuhalten, dass, wenn Aufzeichnungen einen derart tiefen Einblick in höchst intime innerpsychische Vorgänge erlauben, wie dies im zitierten Urteil geschehen ist, ein staatlicher Zugriff darauf als nicht verhältnismässig beurteilt werden muss und dies ungeachtet der damit verfolgten Ziele, womit die Voraussetzungen für die Anerkennung als Kerngehalt erfüllt wären.<sup>154</sup>

Neuerdings versucht auch SCHWEIZER mit Bezug auf andere Autoren den Kerngehalt der informationellen Selbstbestimmung zu umreissen. Danach werden folgende Konstellationen als mögliche Kerngehaltsverletzungen festgehalten: Wenn das Recht auf Zugang zu den eigenen Daten gänzlich ausgeschlossen werden könnte, wenn man sich einer Überwachung im öffentlichen Raum nicht entziehen könnte, wenn so viele Daten über eine Person erhoben würden, dass diese «durchsichtig» werde oder wenn Daten über gewisse Vorgänge der Intimsphäre gesammelt und bearbeitet würden.<sup>155</sup> Ein verallgemeinerbarer Kerngehalt lässt sich aus dem Dargestellten zwar wohl (noch) nicht definieren, immerhin lässt sich jedoch ein Umriss eines Kerngehalts des Rechts auf informationelle Selbstbestimmung erahnen.

---

<sup>153</sup> BVerfGE 80, 367 (381).

<sup>154</sup> SCHEFER, Kerngehalte, S. 448.

<sup>155</sup> SCHWEIZER, SG-Komm BV, N 83 zu Art. 13 BV.

### **3.5 Fazit**

Die vorangehenden Ausführungen zeigen, dass die Lehre nach wie vor davon ausgeht, dass es sich beim Recht auf informationelle Selbstbestimmung um ein verfassungsmässiges Recht handelt. Und obwohl es zum Teil einige Mühe bereitete, eine herrschende Lehre in Bezug auf die einzelnen grundrechtlichen Determinanten Schutzzweck, Grundrechtsträger, sachlicher Schutzbereich und Kerngehalt ausfindig zu machen sei es mangels klarer Statements oder weil die einzelnen Auffassungen stark divergieren so konnte eine solche am Ende doch noch eruiert werden: Demnach liegt der Schutzzweck in der Gewährleistung der Möglichkeit, die eigene Persönlichkeit und damit verbunden die sozialen Rollen und Beziehungen (mit) zu definieren und zu wahren, um dadurch ein selbstbestimmtes Verhalten zu ermöglichen. Zu diesem Zweck wird die Entscheidungsfreiheit über die eigenen Daten und Informationen aller natürlichen und juristischen Personen des Privatrechts geschützt, sofern Letztere betreffende Daten und Informationen ein Verletzungspotential für ihre Persönlichkeit aufweisen. Auch der Dunstkreis eines Kerngehaltes konnte ausgemacht werden, in Fällen höchst intimer Bezeugungen, deren Verwendung, gleichgültig zu welchem Zweck, die Menschenwürde in Frage stellt.

## **4 Résumé und Überleitung**

Die in diesem Kapitel nachgezeichnete Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung durch Rechtsprechung, Bundesgesetzgeber und Lehre gibt ein heterogenes Bild ab: Rechtsprechung und Lehre tun sich äusserst schwer damit, konkrete Aussagen zum Bestand, zum Umfang und zur Reichweite des Grundrechts auf informationelle Selbstbestimmung zu machen, welche teilweise auch noch stark divergieren. Vom Bundesgesetzgeber hätte immerhin beim Erlass des DSG erwartet werden können, dass er das Konstrukt der informationellen Selbstbestimmung zumindest im Hinterkopf behält. Letztlich ist es aber auch ihm äusserst schwer gefallen, eine konkrete Position zu beziehen. Dies führte einerseits dazu, dass das DSG der gesetzgeberischen Intention – das Selbstbestimmungsrecht in Bezug auf die persönlichen Daten zu stärken – nicht gerecht wurde, andererseits tut sich aber auch ein gewisser Wertungswiderspruch auf, da die Art. 179 ff. StGB zumindest den Anschein erwecken, dieser Idee zu folgen. Immerhin konnte aus den



### III Umsetzung in Rechtsprechung, Lehre und Bundesrecht

dargelegten Auffassungen und Überlegungen eruiert werden, dass ein verfassungsmässiges Recht des einzelnen in Bezug auf seine Daten und Informationen besteht, und auch, wie dieses Recht aussehen soll.

Dieses eruierte Verständnis des Rechts auf informationelle Selbstbestimmung ist jedoch keinesfalls unbestritten. Bereits bei der Übernahme des Konstrukts aus Deutschland wurde harsche Kritik am Bundesgericht geübt und die Kritikpunkte haben mit zunehmender Implementierung des Grundrechts nur zugenommen. Ein Beharren auf diesem Verständnis, ohne die Kritikpunkte zu beleuchten und zu würdigen, wäre für den Umgang mit den sich im Bereich der modernen Datenbearbeitung stellenden Probleme ein Fehler und dem Recht an und für sich nur abträglich. Nachfolgend wird es deshalb darum gehen, die eindringlichsten Kritikpunkte und die augenscheinlichsten Schwachstellen am herrschenden Verständnis des Grundrechts auf informationelle Selbstbestimmung zu beleuchten und zu würdigen, um daraus Schlüsse für den künftigen Umgang mit dem Grundrecht zu gewinnen.

## IV Kritik am herrschenden Verständnis und deren Würdigung

### 1 Herkunft – Unterschied zwischen der deutschen und der schweizerischen Rechtsordnung

Der erste kritische Einwand gegen ein Recht auf informationelle Selbstbestimmung, wie es zuvor skizziert wurde, richtet sich gegen die unreflektierte Übernahme aus einer fremden Rechtsordnung. Die Konstruktion des informationellen Selbstbestimmungsrechts stammt aus Deutschland, wo sie im Rahmen der allgemeinen Handlungsfreiheit entwickelt wurde.<sup>156</sup> Diese allgemeine Handlungsfreiheit gibt jedem Menschen das Recht auf freie Entfaltung seiner Persönlichkeit, sofern er dabei nicht die Rechte anderer verletzt und nicht gegen die verfassungsmässige Ordnung oder das Sittengesetz verstösst (Art. 2 Abs. 1 GG). Geschützt ist damit nicht nur ein begrenzter Bereich der Persönlichkeitsentfaltung, sondern jede Form menschlichen Handelns ohne Rücksicht darauf, welches Gewicht der Betätigung für die Persönlichkeitsentfaltung zukommt. Damit kommt der *allgemeinen Handlungsfreiheit* nach deutschem Recht eine weitaus grössere Reichweite zu als dem Schweizer Äquivalent der *persönlichen Freiheit*. Das Grundrecht auf persönliche Freiheit, welches hierzulande als Grundgerüst für die informationelle Selbstbestimmung dienen musste, schützt anders als die allgemeine Handlungsfreiheit nur die *elementaren Erscheinungen der Persönlichkeitsentfaltung*,<sup>157</sup> so beispielsweise den Wunsch nach Kindern,<sup>158</sup> eine allgemeine Handlungsfreiheit wurde vom Bundesgericht zu keiner Zeit als Ausfluss der persönlichen Freiheit anerkannt.<sup>159</sup> Ein umfassendes Selbstbestim-

---

<sup>156</sup> AEBI-MÜLLER, RZ 595 f.

<sup>157</sup> AEBI-MÜLLER, RZ 595.

<sup>158</sup> BGE 119 Ia 460 ff.

<sup>159</sup> M.w.H. MÜLLER/SCHEFER, S. 141; statt vieler BGE 130 I 369 ff (373), E. 2, BGE 116 Ia 420 ff. (422), E. 2a.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

mungsrecht ist dem Schweizer Persönlichkeitsschutz somit fremd und passt damit bereits von dessen Konzeption her nicht in die schweizerische Rechtslandschaft.<sup>160</sup>

Die unkritische und unreflektierte Übernahme des Konstrukts der informationellen Selbstbestimmung durch das Bundesgericht stellt fraglos einen schwerwiegenden Mangel in Bezug auf das Grundrecht dar und erschwert die rechtliche Auseinandersetzung damit auf unnötige Art und Weise. Könnte davon ausgegangen werden, dass sich das Bundesgericht bei der Einführung des Konzepts der informationellen Selbstbestimmung mit dem diesem zugrundeliegenden Grundrecht, dessen Schutzbereich und Schranken vertieft auseinandergesetzt hätte und seine Entscheidung, dieses Grundrecht in der Schweiz einzuführen, in Kenntnis und unter Berücksichtigung dieser Divergenzen getroffen hätte, vermöchte dies die Kritik eventuell ein wenig zu schmälern. Es ist aber immerhin zu bemerken, dass auch das deutsche Recht Relativierungen des umfassenden Selbstbestimmungsrechts kennt. So werden nur erhebliche Eingriffe in die allgemeine Handlungsfreiheit als grundrechtsrelevant verstanden; Bagatellen werden nicht als Eingriff in deren Schutzbereich angesehen. Darüber hinaus wird die freie Entfaltung der Persönlichkeit nur im Rahmen der verfassungsmässigen Ordnung, der Rechte anderer und des Sittengesetzes garantiert.<sup>161</sup> Da diese Vorbehalte den Schutzbereich jedoch nicht auf das gleiche Mass reduzieren, wie dem der persönlichen Freiheit, hat dieser Kritikpunkt wohl weiterhin Bestand.

## 2 Konturlosigkeit und Inhaltsleere

Von den Verfechtern einer reinen Wortlautinterpretation des Art. 13 Abs. 2 BV wird vorgebracht, dass die Folge der Befürwortung eines Rechts, selbst bestimmen zu können, wer was wann über einen weiss, ein inhaltsleeres Selbstbestimmungsrecht mit einem konturlosen Schutzbereich sei.<sup>162</sup> Die Bestimmung beschreibe weder das

---

<sup>160</sup> Vgl. GÄCHTER/EGLI, RZ 24.

<sup>161</sup> <http://www.grundrechtenschutz.de/gg/freie-entfaltung-der-personlichkeit-258> (zuletzt besucht am 10.4.2014).

<sup>162</sup> GÄCHTER/EGLI, RZ 28.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

Schutzobjekt noch den Schutzzweck eines Grundrechts auf informationelle Selbstbestimmung überzeugend.<sup>163</sup>

Das Argument der Konturlosigkeit kann wohl nicht von der Hand gewiesen werden, bereitet die Konkretisierung des von der herrschenden Lehre vertretenen Anspruchs auf Selbstbestimmung bezüglich der eigenen Daten und Informationen doch auf allen Ebenen Mühe. Dennoch geht der Vorwurf der Inhaltsleere der hier vertretenen Ansicht nach zu weit. Allein das Wesen der informationellen Selbstbestimmung im Sinne einer allgemeinen Handlungsfreiheit in Bezug auf die eigenen Daten und Informationen macht den Anspruch noch nicht inhaltsleer. Auch die Eigentumsgarantie nach Art. 26 BV ist ihrem Wesen nach eine Art allgemeine Handlungsfreiheit, und dennoch wird ihr deshalb nicht der Vorwurf der Inhaltsleere entgegen gehalten. Natürlich stellen sich im Kontext der informationellen Selbstbestimmung andere, ja viel grundsätzlichere Probleme als bei der Eigentumsgarantie: Bereits die Fragen, was denn überhaupt der eigenen Dispositionsfreiheit unterliegt, wie dieses Etwas abgegrenzt und durchgesetzt werden kann etc., sind in Bezug auf die komplexen Gebilde Daten/Information schwierig zu beantworten. Inhaltsleere bedeutet es dennoch nicht, da herrschende Lehre und bundesgerichtliche Rechtsprechung doch zumindest in Grundzügen zu umschreiben vermögen, welche Ansprüche vom Schutz des Grundrechts gedeckt sind und diese Grundzüge wiederum zumindest gewisse Überschneidungen vorweisen. So sind beispielsweise die Ansprüche auf Berichtigung falscher Daten, auf Löschung ungeeigneter und nicht oder nicht mehr benötigter Daten und auf Auskunft bzw. Einsicht unbestrittene Gehalte der informationellen Selbstbestimmung, womit dieser Kritikpunkt nur teilweise standhält.

### 3 Ein de facto-Informationsverbot

Als weiteres Problem des Grundrechts auf informationelle Selbstbestimmung wird ins Feld geführt, dass der Betroffene kein Interesse an der Unterlassung einer Datenbearbeitung darlegen müsse. Vielmehr sei es der Datenbearbeiter, der die Zulässigkeit der Datenbearbeitung durch einen Rechtfertigungsgrund nachweisen müsse.<sup>164</sup>

---

<sup>163</sup> BELSER, Datenschutzrecht, § 6 N 118, GÄCHTER/EGLI, RZ 36.

<sup>164</sup> AEBI-MÜLLER, RZ 597.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

Schranken des informationellen Selbstbestimmungsrechts würden somit erst auf der *Ebene der Rechtfertigung* eingeführt,<sup>165</sup> eine von Beginn weg zulässige Datenbearbeitung gegen den Willen des Betroffenen existiere in diesem Modell nicht. Dies wiederum führe de facto zu einem Informationsverbot, indem jedes personenbezogene Datum zum *absoluten Recht* werde.<sup>166</sup> Jeder staatliche Umgang mit Personendaten, jede noch so minimale Erhebung von Informationen, die einen Persönlichkeitsbezug aufweisen, erscheine insoweit als Grundrechtseingriff, wäre also grundsätzlich verboten, sofern er nicht über Art. 36 BV gerechtfertigt werden könne.<sup>167</sup>

Bei der herrschenden Vorstellung eines Rechts auf informationelle Selbstbestimmung handelt es sich tatsächlich um ein *Freiheitsrecht*, welchem immanent ist, dass Eingriffe in dessen Schutzbereich nur zulässig sind, wenn die *Voraussetzungen von Art. 36 BV* erfüllt sind. Dies führt der hier vertretenen Meinung nach jedoch nicht zu einem Informationsverbot, kann der Gesetzgeber doch den Rahmen bestimmen, in dem eine Datenbearbeitung (sei es durch den Staat oder durch Private) – auch gegen den Willen des Betroffenen – zulässig ist, was er übrigens bereits vielfach getan hat.<sup>168</sup> Natürlich lässt sich in diesem Zusammenhang nicht von der Hand weisen, dass es für den Gesetzgeber eine grosse Herausforderung darstellt, für jede von ihm als notwendig erachtete Datenbearbeitung eine Rechtsgrundlage zu schaffen.<sup>169</sup> Aber genau dies ist doch letztlich eines der tragenden Fundamente unseres Staatsverständnisses: Der Staat handelt nicht einfach, weil er der Staat ist, sondern weil er in Form eines rechtsetzenden Erlasses vom Souverän die Erlaubnis oder Pflicht dazu hat. Staatliche Datenbearbeitungen, mögen sie auch noch so nebensächlich erscheinen, tangieren, wie noch vertieft zu zeigen sein wird, unsere Persönlichkeit, tangieren das Grundrecht auf informationelle Selbstbestimmung. Erachtet es der Ge-

---

<sup>165</sup> AEBI-MÜLLER, RZ 597.

<sup>166</sup> AEBI-MÜLLER, RZ 597.

<sup>167</sup> GÄCHTER/EGLI, RZ 28.

<sup>168</sup> Anstatt vieler: Art. 66c Abs. 1 IVG, welcher es der IV-Stelle erlaubt, fahruntüchtige Personen der zuständigen kantonalen Behörde zu melden, Art. 42 Abs. 3 KVG, welcher u.a. Spitäler verpflichtet Personendaten, welche benötigt werden, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können, an die Krankenversicherungen bekannt zu geben; Art. 170 Abs. 1 ZGB, welcher den Ehegatten verpflichtet, seinem Partner das Einkommen offen zu legen.

<sup>169</sup> Zur vertieften Erörterung dieser Problematik siehe Kapitel IV, Ziffer 5.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

gesetzgeber als notwendig, dies zu tun, dann hat er auch die Pflicht, in einem rechtsetzenden Erlass festzuhalten, was und wozu er dies tut. Und selbst wenn der Gesetzgeber jegliches Datenbearbeiten regeln könnte, muss immer noch die Frage in den Raum gestellt werden, welchen Voraussetzungen die Rechtsgrundlagen genügen müssen, damit es faktisch nicht zu einem Aushöhlen des Grundrechtsschutzes kommt. So ist beispielsweise darauf zu achten, dass Erlasse, welche Datenbearbeitungen regeln, genügend bestimmt sind.<sup>170</sup> Es wäre dem Schutz der Persönlichkeit nicht geholfen, wenn der Staat am Ende jegliche Datenbearbeitung durchführen dürfte, weil er sich durch unbestimmte Erlasse die Rechtfertigung dazu gibt.<sup>171</sup> Das Beschriebene gilt unter anderen Vorzeichen auch für Privatpersonen: Es ist in Anbetracht der noch zu erörternden Gefahren für die Persönlichkeit durch die Bearbeitung personenbezogener Daten und Informationen nicht einzusehen, weshalb es zulässig sein soll, dass Privatpersonen persönliche Daten grundsätzlich *ohne Rechtfertigungsgrund* bearbeiten dürfen.<sup>172</sup> Und selbst das Konstrukt der *Einwilligung* hilft oft nur wenig, wenn der Betroffene aufgrund der Komplexität der Sache nicht fassen kann, wozu er überhaupt einwilligt, oder am Ende in so viele Datenbearbeitungen eingewilligt hat, dass er gläserner dasteht, als er dies je wollte. Die Kritik eines de facto-Informationsverbot scheint nach dem Dargelegten als unzutreffend.

#### **4 Grundrechtskollision / Verletzung des Grundsatzes der Gleichrangigkeit der Grundrechte**

Im Weiterzug der Kritik des de facto-Informationsverbots könnte ferner beanstandet werden, dass bei konsequenter Befürwortung eines Rechts auf informationelle Selbstbestimmung, diesem im Rahmen einer Grundrechtskollision immer der Vorrang zu geben ist, da sonst gar keine echte Selbstbestimmung möglich ist, was jedoch wiederum im Widerspruch zum Grundsatz der Gleichrangigkeit der Grundrechte steht.

---

<sup>170</sup> Siehe zum Grad der erforderlichen Bestimmtheit SIGRIST, S. 151 ff.

<sup>171</sup> Vgl. DRUEY, Strukturelle Schwächen, S. 146.

<sup>172</sup> Zu den Gefahren für die Persönlichkeit siehe Kapitel V, Ziffer 5.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

Eine Grundrechtskollision dürfte vor allem zum Recht auf Information (Art. 16 Abs. 2 BV) oder zum Recht auf Forschungsfreiheit (Art. 20 BV) auftreten. Die *Informationsfreiheit* garantiert das Recht, Meinungen und Nachrichten ohne behördliche Eingriffe zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und sie sodann weiter zu verbreiten.<sup>173</sup> Die Empfangsfreiheit schützt dabei das Recht, alle über den Äther ausgestrahlten und für die Öffentlichkeit bestimmten Nachrichten und Programme zu empfangen. Der grundrechtliche Anspruch auf aktives Beschaffen von Informationen bezieht sich denn auch nur auf allgemein zugängliche Quellen. Die allgemeine Zugänglichkeit einer Quelle bestimmt sich dabei nach den anwendbaren gesetzlichen oder verfassungsrechtlichen Bestimmungen.<sup>174</sup> Es besteht somit kein allgemeines Recht, sämtliche Informationen zu empfangen, zu beschaffen oder weiter zu verbreiten. Insoweit besteht gar keine Kollision, da das Grundrecht auf Information einzig einen Anspruch auf Empfang der für die Öffentlichkeit bestimmten Informationen und auf das Beschaffen aus öffentlich zugänglichen Quellen normiert und davon ausgegangen werden kann, dass solche Informationen von den Betroffenen in selbstbestimmter Weise öffentlich zugänglich gemacht wurden. Schwierigkeiten ergeben sich hier vor allem in praktischer Hinsicht unter dem Blickwinkel von Onlineplattformen wie beispielsweise Facebook, wo sich u.a. die Frage stellt, ob eine 350 Freunden zugänglich gemachte Information noch als privat oder bereits als öffentlich zu qualifizieren ist.<sup>175</sup>

Bei der *Forschungsfreiheit* ist die Kollision jedoch bereits auf theoretischer Sicht leicht ersichtlich: Auf der einen Seite steht das Interesse des Betroffenen, über seine persönlichen Daten und Informationen selbst zu bestimmen, auf der anderen Seite wünscht beispielsweise die Krebsforschung den Zugang zu so vielen Personendaten wie möglich, und dies aus ganz persönlichen Bereichen. Dem Recht des Betroffenen auf Selbstbestimmung stehen hier gleich zwei entgegenstehende Interessen gegenüber: Das Interesse des Forschers an der Forschung an und für sich, aber auch das Interesse der Gesellschaft am Erkenntnisgewinn aus dieser Forschung. Laut Bundesgericht sind diese entgegenstehenden Interessen nun nach dem Prinzip der *prak-*

---

<sup>173</sup> KLEY/TOPHINKE, SG-Komm BV, N 34 zu Art. 16 BV.

<sup>174</sup> KLEY/TOPHINKE, SG-Komm BV, N 36 f. zu Art. 16 BV.

<sup>175</sup> Zur Diskussion, wann etwas als öffentlich gilt, siehe Kapitel III, Ziffer 2.1.2.2.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

*tischen Konkordanz* in einen möglichst schonenden Ausgleich zu bringen. Allein schon diese Formulierung weist darauf hin, dass so etwas wie ein übergeordnetes Grundrecht von der Rechtsprechung nicht akzeptiert würde.

Die aufgeworfene Kritik, wonach bei konsequenter Befürwortung eines informationellen Selbstbestimmungsrechts, diesem im Rahmen einer Grundrechtskollision immer der Vorrang zu geben ist und es aufgrund dessen zu einer Verletzung des Prinzips der Gleichrangigkeit der Grundrechte kommt, ist deshalb gleichzeitig richtig und falsch: Ein umfassendes Dispositionsrecht über die eigenen Daten und Informationen führt unausweichlich an die Grenzen anderer Grundrechte und könnte nur dann konsequent durchgesetzt werden, wenn das andere Recht zurücktritt. Die Ausübung eines jeden Grundrechts führt jedoch früher oder später an die Grenzen eines anderen Grundrechts und könnte nur konsequent durchgesetzt werden, wenn das andere Recht zurück treten würde. Dies ist keine Eigenheit der informationellen Selbstbestimmung, findet etwa die Forschungsfreiheit auch ihre Grenzen an der Religionsfreiheit von Art. 15 Abs. 2 BV. Kein Grundrecht gilt absolut. Jeder dieser grundlegenden Ansprüche kann nach den Voraussetzungen von Art. 36 BV eingeschränkt werden, wobei dessen zweiter Absatz die Grundrechte Dritter explizit erwähnt. Vorhersehbare Grundrechtskollisionen müssen demnach vom Gesetzgeber geregelt werden, sofern er sicherstellen will, dass einem Recht in einer bestimmten Situation der Vorrang zukommt. Dies hat er beispielsweise im Bereich der Forschung u.a. mit dem neuen Humanforschungsgesetz getan, welches präzise vorschreibt, wann und unter welchen Umständen dem Recht auf Forschung oder dem Recht auf informationelle Selbstbestimmung der Vorrang zu geben ist.<sup>176</sup>

## 5 Realisierbarkeit

Eine der wohl herausforderndsten und damit bedeutendsten Schwierigkeiten in Bezug auf die informationelle Selbstbestimmung stellt die *praktische Umsetzung* dieses Grundrechts dar. Das von der herrschenden Lehre und vorwiegend in der Rechtspre-

---

<sup>176</sup> So sieht etwa Art. 4 HFG vor, dass das Wohlergehen des einzelnen Menschen Vorrang gegenüber den Interessen der Wissenschaft und der Gesellschaft hat, Art. 7 HFG sieht den Grundsatz der Einwilligung vor, demgegenüber beispielsweise Art. 30 Abs. 2 HFG vorsieht, wann von diesem Grundsatz im Interesse der Forschung abgewichen werden darf.



#### IV Kritik am herrschenden Verständnis und deren Würdigung

chung postulierte Dispositions- oder Entscheidungsrecht des einzelnen über sämtliche ihn betreffenden Daten muss in dieser Absolutheit als schlicht nicht realisierbar bezeichnet werden: Zum einen ist es in der heutigen vernetzten Zeit für den einzelnen unmöglich zu erkennen, wer wann welche Daten über ihn bearbeitet. Dies gilt nicht nur unter Privaten, wo die Grundrechte, je nach Meinung, ohnehin nur indirekt zum Zuge kommen (siehe zur Horizontalwirkung von Grundrechten Kapitel VI, Ziffer 2), sondern auch bei der *staatlichen Bearbeitung* der eigenen Personendaten. Von Gesetzes wegen gilt zwar das Prinzip der Transparenz (Art. 4 Abs. 4 DSGVO). Alleine die riesige Zahl der Daten verunmöglicht es aber der betroffenen Person, einen Überblick zu erhalten, geschweige denn das Ausmass dieser Datenbearbeitungen zu erfassen. Bei *privaten Datenbearbeitern* potenzieren sich die Möglichkeiten der Verwendung noch um ein Vielfaches, da de facto keinerlei wirksame Kontrolle in diesem Bereich herrscht und in Anbetracht der riesigen Datenmengen wohl auch gar nicht umfassend existieren könnte. Es kann etwas überspitzt formuliert behauptet werden, dass es eher einem Zufall gleicht, wenn der einzelne erfährt, dass jemand den Schutzbereich seines Grundrechts auf informationelle Selbstbestimmung tangiert. Zum anderen stellt es für den Gesetzgeber eine grosse Herausforderung dar, für jede staatliche Datenbearbeitung und damit jeden Grundrechtseingriff durch öffentliche Organe eine gesetzliche Grundlage als Rechtfertigung im Sinne von Art. 36 Abs. 1 BV zu schaffen. Die Vielfalt an Sachverhalten und Entwicklungen machen es ihm schwer, heute die Datenbearbeitungen von morgen vorherzusehen und die dafür unter dem Blickwinkel der künftigen Realität adäquaten Rechtsgrundlagen zu erarbeiten. Dieses Dilemma führt nicht selten zur Schaffung von unbestimmten Rechtsnormen, welche kaum Aussagegehalt aufweisen und damit für den Grundrechtsschutz weder von heute noch von morgen dienlich sind.<sup>177</sup>

Darüber hinaus ist es wenig realistisch davon auszugehen, dass jeder private Datenbearbeiter sich tatsächlich seiner Pflichten im Umgang mit Personendaten bewusst ist (zumindest ist dies heute noch nicht der Fall). Und selbst wenn er sich dessen bewusst wäre, bedeutet dies noch nicht, dass er ihnen auch nachkommt. Eine ganzheitliche Durchsetzung des Grundrechts auf informationelle Selbstbestimmung ist,

---

<sup>177</sup> Zur Aushöhlung des Grundrechtsschutzes durch Schaffung von Rechtsgrundlagen als Rechtfertigungsgründe siehe Kapitel IV, Ziffer 3.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

wie die gemachten Ausführungen gezeigt haben, schlicht nicht realistisch. Dieser Tatsache lässt sich nur mit einer weiteren entgegen: Kein Grundrecht kann für sich die 100% Realisierbarkeit beanspruchen. Solange die Rechtsordnung den Menschen Regeln für deren Zusammenleben vorschreibt, wird es immer wieder Personen geben, die sich nicht daran halten oder nach Umgehungsmöglichkeiten suchen. Dies stellt aber freilich noch keinen ausreichenden Grund dar, um das Grundrecht an und für sich in Frage zu stellen. Schliesslich «fungieren die Grundrechte nicht als rechtliche Sicherung einer <natürlichen> Freiheit oder real schon vorhandener Chancen.»<sup>178</sup> Vielmehr geht es darum, dass die betroffene Person überhaupt in Bezug auf Geschehnisse ausserhalb ihres faktisch vorhandenen Einfluss- und Kenntnisbereiches geschützt wird.<sup>179</sup> Insoweit kann festgehalten werden, dass die Kritik der fehlenden Realisierbarkeit durchaus berechtigt ist, sie ist jedoch insoweit zu relativieren, als dieser Kritikpunkt sicherlich für die meisten Grundrechte gilt.

### **6 Ist Selbstbestimmung in Bezug auf Informationen überhaupt möglich?**

Mit dem Kritikpunkt bezüglich der mangelnden Realisierbarkeit eng verbunden ist die Frage, ob informationelle Selbstbestimmung, also Selbstbestimmung in Bezug auf persönliche Informationen und Daten, überhaupt möglich ist. Im Unterschied zum vorangehenden Kritikpunkt geht es bei der Beantwortung dieser Frage jedoch nicht um die praktische Umsetzung des von Gesetzgeber, Lehre, Rechtsprechung und letztlich auch der Gesellschaft geforderten Minimums, wie das Vorhandensein einer Rechtfertigung für den Grundrechtseingriff oder das Vorhandensein von Transparenz als Voraussetzung für die Durchsetzbarkeit des grundrechtlichen Anspruchs. Im Nachfolgenden geht es vielmehr um die grundlegenden Fragen, wie was ist Selbstbestimmung? Was sind Informationen? Was sind Daten? und letztlich: Ist Selbstbestimmung bezüglich Informationen oder Daten überhaupt möglich? Die Beantwortung dieser Fragen ist zentral, denn würde sie negativ ausfallen, würde dies die Existenzberechtigung der informationellen Selbstbestimmung in Frage stellen.

---

<sup>178</sup> ALBERS, Informationelle Selbstbestimmung, S. 132.

<sup>179</sup> ALBERS, Informationelle Selbstbestimmung, S. 132.

### 6.1 Was ist Selbstbestimmung?

#### 6.1.1 Errungenschaft der Aufklärung

Der Begriff der «Selbstbestimmung» und das ihm zugrundeliegende Menschenbild haben ihren Ursprung in einer Zeit, in der sich die Menschen von der Bevormundung durch religiöse und weltliche Obrigkeiten zu lösen begonnen haben und dazu angehalten wurden, sich ihres eigenen Verstandes zu bedienen.<sup>180</sup> Die Selbstbestimmung des einzelnen wurde darin erblickt, sich von fremden Vorstellungen und Vorgaben los zu sagen und frei, nur gestützt auf den eigenen Verstand, seine Handlungen zu bestimmen. Der in Folge dieser Neuanschauung aufgeklärte Mensch sollte nicht mehr nach den Vorstellungen der Kirche, weltlichen Herren oder sonst hoch angesehenen Leuten leben,<sup>181</sup> sondern aus «seiner selbstverschuldeten Unmündigkeit»<sup>182</sup> ausbrechen und sein Leben eigenverantwortlich und somit selbstbestimmt an die Hand nehmen.<sup>183</sup> «*Sapere aude!* Habe Mut, dich deines eigenen Verstandes zu bedienen! ist also der Wahlspruch der Aufklärung.»<sup>184</sup> Es überrascht daher wenig, dass «*Autonomie*» als Synonym für Selbstbestimmung mit «das sich selbst gebende Gesetz» übersetzt werden kann.<sup>185</sup> Eine autonome Person ist demzufolge in der Lage, ihre Handlungen aus freien Stücken zu bestimmen.

---

<sup>180</sup> KANT, S. 481.

<sup>181</sup> Vgl. MÜLLER MARKUS, Selbstbestimmung, S. 65.

<sup>182</sup> «Es ist so bequem, unmündig zu sein. Habe ich ein Buch, das für mich Verstand hat, einen Seelsorger, der für mich Gewissen hat, einen Arzt, der für mich die Diät beurteilt usw., so brauche ich mich ja nicht selbst zu bemühen. Ich habe nicht nötig zu denken, wenn ich nur bezahlen kann; andere werden das verdrießliche Geschäft schon für mich übernehmen. Dass der bei weitem größte Teil der Menschen (darunter das ganze schöne Geschlecht) den Schritt zur Mündigkeit, außer dem dass er beschwerlich ist, auch für sehr gefährlich halte, dafür sorgen schon jene Vormünder, die die Obergewalt über sie gütigst auf sich genommen haben».  
(KANT, S. 481).

<sup>183</sup> KANT, S. 481.

<sup>184</sup> KANT, S. 481.

<sup>185</sup> RITSERT, S. 14.

##### 6.1.2 Grundvoraussetzung menschlicher Interaktion

Es wäre jedoch anmassend davon auszugehen, dass die Menschen vor dem Zeitalter der Aufklärung keine Autonomie besessen hätten. Wir müssen davon ausgehen, dass seit dem Tag, als Menschen mit anderen Menschen zu interagieren begonnen und Beziehungen geknüpft haben, sie unbedarft davon ausgegangen sind, dass ihr Gegenüber selbstbestimmt handelt, es seine Handlungen also nicht durch einen anderen dirigieren lässt. Ohne diese Annahme hätte sich kein Vertrauen bilden können und Beziehungen zu anderen Menschen wären nicht eingegangen worden. Diesem Verständnis zufolge ist die Selbstbestimmung ein *zentrales Element* unseres menschlichen Selbstverständnisses, quasi eine Grundhaltung anderen Menschen gegenüber und somit eine Grundvoraussetzung menschlicher Interaktion. Insofern kann die Selbstbestimmung als etwas Ausser-Rechtliches, etwas *dem Menschen Inhärentes* angesehen werden, das schon immer in ihm steckte und das er zur Verwirklichung seines – egal wie gearteten – Lebens bedarf.<sup>186</sup> Es mag kritische Stimmen geben, die hier einwenden könnten, dass es sich genau umgekehrt verhalte und es der Staat, mitunter das Recht sei, welcher die Selbstbestimmung des einzelnen erlaube oder eben nicht. Diesen Kritikern müsste zweierlei entgegen gehalten werden: Zum einen ist der einzelne auch in einem totalitären Staat, der dem Bürger kaum eine Handlungsbefugnis zugesteht, immer noch «frei» zumindest eine selbstbestimmte Handlung zu tun, und zwar seinem Leben ein Ende zu setzen. Zum anderen ist zu konstatieren, dass wir gar nicht in der Lage wären, den Begriff «Recht» zu schaffen, ohne auf die Selbstbestimmung zu referenzieren.<sup>187</sup> Ohne den Glauben und das Vertrauen an und in die Existenz der Selbstbestimmung wären auch andere Begriffe wie Moral oder Verantwortung nicht ausgebildet worden.<sup>188</sup> Als Beispiel, wie sich das Recht auf diese Annahme stützt, ist die vor allem im Strafrecht angewendete *Maxime der Schuldfähigkeit* zu nennen. Wenn der Richter keinen freien Willen, also keinen Vorsatz für die begangene Tat nachweisen kann, muss sein Urteil unserer Rechtsauffassung nach weniger scharf ausfallen.<sup>189</sup> Auch die *schweizerische*

---

<sup>186</sup> HIMMELMANN, S. 325.

<sup>187</sup> Vgl. HIMMELMANN, S. 325.

<sup>188</sup> Vgl. HIMMELMANN, S. 325.

<sup>189</sup> RITSERT, S. 13.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

*Bundesverfassung* verfolgt in ihrer Ausgestaltung hartnäckig das Bild vom *selbstbestimmten Bürger*, indem sie dem Menschen möglichst umfassend jene Freiheiten gewährleistet, welche ihm eine «vernunftgeleitete Selbstbestimmung und Selbstentfaltung erlauben.»<sup>190</sup> Ja sogar unser Staatsverständnis einer freien Demokratie geht von einem selbstbestimmten Menschenbild aus, das dem Menschen die Fähigkeiten zugesteht, «zwischen den verschiedenen gegensätzlichen Auffassungen zu unterscheiden, unter den Meinungen auszuwählen, Übertreibungen als solche zu erkennen und vernunftgemäss zu entscheiden.»<sup>191</sup> Es ist offensichtlich, dass sowohl im zwischenmenschlichen Zusammenleben als auch im Recht und in der Politik beharrlich von der Annahme ausgegangen wird, dass wir Menschen in entscheidender Hinsicht aus eigener Bestimmung handeln und wir genau deswegen für unser Handeln zur Rechenschaft gezogen werden können.<sup>192</sup>

##### 6.1.3 Mensch als vernunftbegabtes Wesen

Gerade diese Vorstellung, dass es sich beim Menschen um ein vernunftbegabtes Wesen handelt, welches voraussichtlich alle Vor- und Nachteile abwägt und darauf gestützt frei und selbstbestimmt eine Entscheidung fällt, wird allerdings – unabhängig von der Frage, ob es sich bei der Selbstbestimmung um ein vom Recht geschaffener oder dem Recht zugrunde liegender Begriff handelt – immer wieder in Zweifel gezogen. Bereits vom Begriff her setze die «Selbstbestimmung» ein «Selbst» im Sinne eines «homogenen Persönlichkeitskerns» voraus, welcher sich im subjektiven Empfinden vom Aussen abgrenze. Ein solcher homogener Kern existiert gemäss MÜLLER aber nicht, da der Mensch in seinen verschiedenen Rollen als Privatperson, Berufsmensch, Staatsbürger etc., jeweils eine andere Ich-Persönlichkeit einnehme, er somit als «Bündel von Ich-Identitäten» bezeichnet werden könne und eben *kein homogenes Selbst* existiere.<sup>193</sup> Die Äusserungen des Selbst seien darüber hinaus nur selten echt, wahr und verlässlich, eben authentisch.<sup>194</sup> Viele Menschen machten anderen,

---

<sup>190</sup> MÜLLER MARKUS, Selbstbestimmung, S. 66.

<sup>191</sup> BGE 98 Ia 73 ff. (80), E. 3b.

<sup>192</sup> Vgl. HIMMELMANN, S. 325.

<sup>193</sup> MÜLLER MARKUS, Selbstbestimmung, S. 69.

<sup>194</sup> MÜLLER MARKUS, Selbstbestimmung, S. 70.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

aber auch sich selbst, zwecks Stabilisierung des eigenen Selbstbildes nur etwas vor.<sup>195</sup> In Bezug auf die Rationalität des Menschen verweist er auf einen kurzen Blick in die Tageszeitung oder die Nachrichten. Dieser würde genügen, um zu erkennen, dass die Idee des vernunftbegabten Menschen, der sich und sein Schicksal vorwiegend nach rationalen Gesichtspunkten bestimmt, nicht der Realität entspreche. Die meisten Entscheidungen würden wir Menschen vielmehr aufgrund von *Emotionen*, *Trieben* oder einem simplen *Bauchgefühl* treffen.<sup>196</sup> Als letzten Punkt stellt MÜLLER den *Freiheitswillen* in Frage. In einer Zeit, in der die Menschen vor lauter Wahlmöglichkeiten schnell überfordert seien, hätten die meisten irgendwann das Bedürfnis, sich von einer beliebigen Autorität leiten zu lassen.<sup>197</sup> Dadurch werde zumindest deutlich: «Der Wille und die Kraft zur echten Selbstbestimmung ist häufig schwach.»<sup>198</sup> Zynisch gesprochen ist die Selbstbestimmung also «nicht der besonnene Akt eines Vernunftwesens, sondern der Akt eines Teil-Ichs, das sich und seine Umwelt gerne belügt, überwiegend von Emotionen und Impulsen getrieben ist und, was seinen Freiheitswillen angeht, bisweilen widersprüchliche und vielschichtige Signale sendet.»<sup>199</sup>

##### 6.1.4 Alltagspsychologisches System

Doch trotz all dieser Widrigkeiten bleibt wohl unbestritten, dass es so etwas wie Selbstbestimmung geben muss und in ihrem ursprünglichsten Sinn wohl auch immer schon gegeben hat. Denn wie bereits erwähnt, geht der Mensch quasi von Natur aus, ohne sich Gedanken darüber zu machen, davon aus, dass sowohl er selbst als auch andere Menschen ihre Handlungen selbst bestimmen. GERHARDT folgt ebenfalls dieser Ansicht, denn trotz aller konstitutiven Eingebundenheit des Menschen in die Gesellschaft und in die Natur, bleibe es letztlich doch immer der *einzelne Mensch*, welcher sein Leben nach seinen eigenen Einsichten führen muss.<sup>200</sup> Interessanterweise sind auch diejenigen Personen, deren wissenschaftliche Weltanschauung mit

---

<sup>195</sup> MÜLLER MARKUS, Selbstbestimmung, S. 70.

<sup>196</sup> MÜLLER MARKUS, Selbstbestimmung, S. 70.

<sup>197</sup> MÜLLER MARKUS, Selbstbestimmung, S. 71.

<sup>198</sup> MÜLLER MARKUS, Selbstbestimmung, S. 71.

<sup>199</sup> MÜLLER MARKUS, Selbstbestimmung, S. 72.

<sup>200</sup> GERHARDT, 83.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

dem Glauben an die Selbstbestimmung eigentlich nicht vereinbar ist, kaum je bereit, die Idee gänzlich aufzugeben. So ist z.B. auch der Wissenschaftler WOLFGANG PRINZ, der die Idee eines freien Willens und somit den Ursprung der Selbstbestimmung mit wissenschaftlichen Überlegungen nicht vereinbar hält, nicht bereit, seine Kinder nicht in unserem «alltagspsychologischen System» zu sozialisieren. Sie sollten sich weiterhin frei fühlen dürfen und sollen versuchen, «ihr Leben so gut wie möglich zu gestalten.»<sup>201</sup>

Bleiben wir also bei der Idee, dass es sich bei der Selbstbestimmung um etwas dem Menschen ursprünglich Anhaftendes handelt. Für die vorliegende Prüfung, ob Selbstbestimmung bezüglich Daten und Informationen möglich ist, ist es jedoch essenziell, dieses Etwas besser verstehen und präziser definieren zu können. Im Folgenden soll deshalb versucht werden, eine Definition der «Selbstbestimmung» zu finden oder zumindest die Voraussetzungen zu klären, welcher sie bedarf.

##### 6.1.5 Voraussetzungen

Als erstes ist zu erwähnen, dass der Begriff «Selbstbestimmung» in nahezu allen Bereichen verwendet wird. Ja, er erlebt sogar gerade eine Hochkonjunktur.<sup>202</sup> KRÄHNKE vermutet aufgrund dieser Bandbreite der auf die Selbstbestimmung referenzierenden Bereiche sogar, dass es für die Verwendung des Wortes keine feststehenden Grenzen gibt.<sup>203</sup> Doch nicht nur aufgrund der verschiedensten Anwendungsbereiche bleibt der Begriff schwammig, sondern auch weil abweichende, sogar völlig gegensätzliche Verständnisse von Selbstbestimmung aufeinanderprallen können. Denn was der eine als eigene, vernünftige Entscheidung auslegt, kann vom anderen durchaus als Anpassung, Beeinflussung oder Fremdbestimmung wahrgenommen werden.<sup>204</sup> Die Unterscheidung liegt im Verständnis, was als *eigener, freier Wille* und somit als Grundlage für die selbstbestimmte Handlung wahrgenommen wird. Der Leser kann sich nun fragen: «Was sollten wir denn sonst haben, wenn nicht unseren eigenen Willen? Wenn ich eine Einsicht oder einen Willen habe, dann ist es ja meine

---

<sup>201</sup> PRINZ, S. 20 ff.

<sup>202</sup> Vgl. KRÄHNKE, S. 9.

<sup>203</sup> KRÄHNKE, S. 9.

<sup>204</sup> KRÄHNKE, S. 11.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

Einsicht oder mein Wille und nicht die oder den eines anderen.» Tatsächlich sind kaum Situationen vorstellbar, in denen jemand nicht seinen eigenen Willen hat. Dies ist etwa dann der Fall, wenn eine Person durch einen besonderen Umstand wie der Einwirkung von Drogen oder einer extremen seelischen Belastung nicht mehr rational denken kann, den üblichen Einfluss auf sich selbst nicht mehr hat.<sup>205</sup> Die Situation muss aber so extrem sein, dass die Person keinen, egal ob rationalen oder irrationalen, Gedanken mehr fassen kann. Denn selbst wenn sie in der Panik erkennt, dass sie von diesem Ort nur noch weg will, ist dieser Wille ihr eigener. Damit der eigene Wille jedoch auch als eigener *freier Wille*<sup>206</sup> bezeichnet werden kann, bedarf es des Vorhandenseins von echten Alternativen. Wer keine Wahl zwischen verschiedenen Möglichkeiten hat, kann keine freie Entscheidung treffen. Der freie Wille zu einem Tun oder Unterlassen besteht eben gerade in der Möglichkeit, dass ich mich auch für das andere entscheiden könnte.<sup>207</sup> Die Willensfreiheit kann aus denselben Gründen verneint werden wie die «Eigenheit» des Willens, also bei Vorliegen eines besonderen Umstandes wie Drogeneinfluss oder einer extremen seelischen Belastung. In solchen Momenten wird der Wille nicht mehr aufgrund eines Abwägungsprozesses der verschiedenen Alternativen gebildet, sondern ein äußerer Einfluss versperrt die Sicht auf andere Möglichkeiten. Es ist dann zwar ein eigener Wille auszumachen, dieser ist jedoch nicht frei. Eine *Zwangssituation* ändert hingegen am freien Willen grundsätzlich nichts. Ein Beispiel: Ein Mann wird unter vorgehaltener Pistole gezwungen, sein Portemonnaie herauszugeben. Sein Wille, das Portemonnaie zu behalten, ändert sich auch durch die Zwangssituation nicht, nur ist das angedrohte Übel von derartiger Schwere, dass er eine Handlung vornimmt (Portemonnaie herausgeben), die nicht dem eigenen freien Willen entspricht. Und selbst wenn die Person in einer Art gezwungen würde, welche es ihr physisch gar nicht erlauben würde anders zu handeln, als man sie zwingt, wäre dies noch immer nicht ihr eigener freier Wille.<sup>208</sup> Anders sieht es erst dann aus, wenn die Zwangssituation bei der betroffenen Person zu einem besonderen Umstand, wie hysterischer Anfall o.ä., führt. Dann fehlt es der Person ganz grundsätzlich an den kognitiven Fähigkeiten einen

---

<sup>205</sup> Vgl. GERHARDT, S. 250 f.

<sup>206</sup> Nicht zu verwechseln mit «freiwillig», was eher ein Synonym für «selbstbestimmt» ist.

<sup>207</sup> Vgl. GERHARDT, S. 244 ff.

<sup>208</sup> WILLASCHEK, S. 92.



#### IV Kritik am herrschenden Verständnis und deren Würdigung

freien Willen zu bilden, dann wird sie quasi in einem Notfallmodus von ihrem Körper gesteuert. Es kann also konstatiert werden, dass der eigene freie Wille eine Grundvoraussetzung für die Selbstbestimmung ist.

Dieser muss jedoch um weitere Voraussetzungen ergänzt werden. Hat eine Person zwar einen eigenen freien Willen, verhält sie sich jedoch nicht dementsprechend, ist ihr Verhalten nicht als selbstbestimmt zu werten, es bedarf einer dem eigenen freien Willen *entsprechenden Handlung*.<sup>209</sup> Als Beispiel sei hier wiederum die Zwangssituation erwähnt: Der Mann hat zwar einen eigenen freien Willen, sein Portemonnaie zu behalten, seine Handlung (die Herausgabe des Portemonnaies) stimmt jedoch nicht mit seinem freien Willen überein, die Handlung war somit nicht selbstbestimmt. Natürlich könnte dagegen argumentiert werden, dass der Mann auch auf die Herausgabe des Geldes hätte verzichten können. Rein theoretisch stand ihm diese Möglichkeit offen, er hatte eine alternative Handlungsmöglichkeit, sein Handeln war frei gewählt und somit selbstbestimmt. In Anbetracht des potentiellen Übels, das ihm der Räuber angedroht hat, muss jedoch festgehalten werden, dass diese Alternative keine adäquate, keine echte ist im Vergleich zur potentiellen Gefahr. Hätte der Räuber dem Mann dagegen Schläge angedroht und Letzterer wäre Boxprofi, dann könnte eher von einer echten Alternative die Rede sein und die Herausgabe des Portemonnaies als freie Handlung betrachtet werden. Frei im Sinne von selbstbestimmt ist eben nicht irgendein Verhalten, irgendeine Wahl, sondern eine, die ich im Bewusstsein von echten Alternativen gewählt habe.<sup>210</sup>

Darüber hinaus ist als dritte Voraussetzung der Selbstbestimmung die *Verfügbarkeit* oder besser die Dispositionsfreiheit zu nennen.<sup>211</sup> Man kann beispielsweise nicht selbstbestimmt darüber entscheiden, ob man wachsen will oder nicht. Selbstbestimmung funktioniert somit nur im eigenen Einflussbereich. Oder anders formuliert:

---

<sup>209</sup> GERHARDT, S. 244 f.

<sup>210</sup> RÖSSLER, S. 99.

<sup>211</sup> Der Begrifflichkeit am nächsten VAN SPYK: «Der Begriff der Dispositionsfreiheit sei demjenigen der Verfügungsfreiheit vorzuziehen, da der zivilrechtliche Begriff der Verfügung i. S. eines Verfügungsgeschäfts impliziere, dass die Verfügungsmacht auf den Erklärungsempfänger übergehe, und damit die Handlungsbefugnis verschoben werde. Insb. die Einwilligung führe jedoch nicht zu einer Verschiebung der subjektiv-rechtlichen Befugnisse vom Erklärenden hin zum Erklärungsempfänger, sondern lediglich zu einer Erweiterung der Befugnisse des Einwilligungsempfängers.» (VAN SPYK, FN 136).

#### IV Kritik am herrschenden Verständnis und deren Würdigung

«Niemand verfügt vollkommen über sich selbst, er bleibt vielmehr an seine psychophysische, sozioökonomische und historische Ausstattung gebunden. (...) Bei entsprechender Anstrengung und dem allemal erforderlichen Glück sind viele Optionen offen – aber stets nur unter den Bedingungen der Realität.»<sup>212</sup>

##### **6.1.6 Fazit**

Obwohl von der Wissenschaft in Frage gestellt, handelt es sich bei der Selbstbestimmung um etwas, von dem der Mensch annimmt, dass er es selbst, aber auch seine Interaktionspartner «besitzen». Insoweit kann von Selbstbestimmung gesprochen werden, wenn eine Person eine Handlung, im Bewusstsein um echte Alternativen, aus eigenem freiem Willen unternimmt und sie im jeweiligen Einflussbereich der betroffenen Person liegt.

## **6.2 Was sind Informationen?**

### **6.2.1 Kein einheitlicher Begriff – kein einheitliches Konzept**

Nach GERHARDT ist Information ein eigenartiges Konstrukt.<sup>213</sup> Erst durch Umwandlung in Materie oder Energie können wir die Information als solche wahrnehmen, was einer der Gründe dafür sein dürfte, dass unter dem Begriff der Information derart Verschiedenes verstanden wird.<sup>214</sup> Die Rechtswissenschaft kennt keinen eigenen oder einheitlichen Begriff der Information.<sup>215</sup> Deshalb muss nachfolgend bei der Begriffsbestimmung darauf aufgebaut werden, was laienhaft oder in anderen Disziplinen als «Information» verstanden wird.

Der Versuch, das Phänomen «Information» aus dem Stegreif zu definieren, ist bereits zum Scheitern verurteilt. Zwar hat jede Person eine Vorstellung, was unter «Information» zu verstehen ist, doch fällt einem bei längerem Überlegen immer noch ein weiterer Aspekt ein, der auch berücksichtigt werden müsste. Die Vielseitigkeit und

---

<sup>212</sup> GERHARDT, S. 146.

<sup>213</sup> MAYER-SCHÖNBERGER, S. 10.

<sup>214</sup> MAYER-SCHÖNBERGER, S. 10.

<sup>215</sup> DRUEY, Information, S. 3.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

die Allgegenwärtigkeit des Phänomens «Information» führen zu einer verwirrenden Anzahl von Definitionsversuchen. Insoweit verwundert es nicht, dass jede Disziplin sich mit einer anderen Facette des Phänomens beschäftigt, so dass eigentlich kein einheitliches Konzept mehr erkennbar ist.<sup>216</sup>

##### 6.2.2 Informationen als Vorgang, Zustand, Inhalt

Beginnen wir deshalb ganz vorne beim Begriff. Das lateinische Wort «informatio» setzt sich zusammen aus «in» und «forma» und bedeutet so viel wie etwas in Form bringen, etwas bilden.<sup>217</sup> Dabei kann «informatio» sowohl den *Vorgang* (also formen, bilden, gestalten, informieren) als auch das Ergebnis dieses Vorgangs bedeuten.<sup>218</sup> Dieses wiederum kann sowohl den *Zustand*, der nach dem Vorgang erreicht wird, sprich das *Informiert-sein*, bedeuten oder aber den *Inhalt* im Sinne eines *Gegenstands*, der vermittelt wurde und weswegen der Zustand des Informiert-seins überhaupt erst erreicht werden konnte.<sup>219</sup> Eben beschriebenes Verständnis von Information liegt uns unbewusst zugrunde, wenn wir davon reden, dass jemand eine wertvolle Information besitzt oder geheime Informationen verkauft hat, etc.<sup>220</sup> So begriffen wird die Information verdinglicht, sie wird zu etwas, mit dem auf irgendeine Weise umgegangen werden kann. DRUEY spricht in diesem Zusammenhang von Reflexen. Seiner Meinung nach sind Informationen etwas Geistiges und als solches nicht fassbar. Nur ihre Reflexe in der körperlichen Welt, also die Art, wie uns Information im Alltag erscheint, können ihr intersubjektive Bedeutung verleihen.<sup>221</sup> Als solche Reflexe kommen dann eben Vorgang, Inhalt oder der Zustand in Frage.<sup>222</sup>

---

<sup>216</sup> Vgl. LOCHMANN, S. 11.

<sup>217</sup> GAUS, S. 29; LOCHMANN, S. 11.

<sup>218</sup> GAUS, S. 29.

<sup>219</sup> Vgl. DRUEY, Information, S. 5.

<sup>220</sup> DRUEY, Information, S. 5.

<sup>221</sup> DRUEY, Information, S. 4.

<sup>222</sup> Vgl. für eine feinere Unterteilung GAUS, S. 29 f.

##### 6.2.3 Information als Inhalt versus Inhalt der Information

Das Recht auf informationelle Selbstbestimmung im Sinne eines Dispositionsrechts des einzelnen lässt sich, wenn überhaupt, nur in Bezug auf eine Sache oder etwas Ähnliches realisieren und nicht in Bezug auf einen Vorgang oder Zustand. Für die vorliegende Arbeit ist demnach nur das Verständnis der Information als Inhalt von Bedeutung. Wenn also im Folgenden von Information gesprochen wird, dann ist immer nur dieser Aspekt des Phänomens gemeint. Gleich vorweg: Information als Inhalt zu begreifen sagt noch nichts über die konkrete *Botschaft* (gemeinläufig der Inhalt der Botschaft) aus, die die jeweilige Information der sie zur Kenntnis nehmenden Person tatsächlich vermittelt. Erst durch die individuellen Vorgänge der Aufnahme und des Verstehens<sup>223</sup> kann die Information eine Wirkung im Sinne einer Bewusstseinerweiterung beim einzelnen hervorrufen.<sup>224</sup> Das «kann» ist hier sehr wichtig, denn ob die Information ein Mehr an Wissen, oder allgemeiner, eine Erweiterung des Bewusstseins, generiert, hängt davon ab, ob der Kenntnisnehmer die Information einerseits als solche deutet und andererseits versteht.<sup>225</sup> Deuten meint decodieren. Eine rote Lampe im Strassenverkehr bedeutet etwa «Halt», in der Schifffahrt «Backbordseite» und im Auto «Warnung».<sup>226</sup> Wenn jemand nun den Code nicht kennt, dann weiss er nicht, dass es sich bei der roten Lampe um eine Information handelt, sondern er sieht einfach eine rote Lampe. Das wirkliche Verstehen der Information hängt aber noch von weiteren Faktoren ab, wie etwa einer gemeinsamen Sprache und einem ähnlichen Wissensstand, auch und besonders bezüglich der jeweiligen Kultur.<sup>227</sup> So kann es einem Schweizer Autofahrer, der erstmals auf deutschen Strassen unterwegs ist, leicht passieren, dass, immer, wenn er auf eine Autobahn einbiegen möchte, doch wieder nur auf einer Hauptstrasse landet, weil die Haupt-

---

<sup>223</sup> ALBERS, Informationelle Selbstbestimmung, S. 95.

<sup>224</sup> DRUEY, Information, S. 4.

<sup>225</sup> Siehe auch GÄCHTER/EGLI, RZ 10 mit Verweis auf ALBERS: «Informationen sind stets Sinnelemente, die in einem bestimmten sozialen Kontext aus Beobachtungen, Mitteilungen oder Daten erzeugt und dann genutzt werden. Mit Bezug auf Daten sind Informationen immer das, was als Aussage eines Datums verstanden wird, d.h. interpretativ ermittelt wird. Die Bedeutung eines Datums erschliesst sich erst mit Blick auf den Verwendungszusammenhang.» (ALBERS, Umgang, RZ 13).

<sup>226</sup> GAUS, S. 30.

<sup>227</sup> GAUS, S. 30.

strassen in Deutschland grün angezeigt sind, während diese Farbe in der Schweiz für die Ausschilderung der Autobahn benutzt wird. Es nützt einem Autofahrer auch nicht viel, wenn er zwar versteht, dass die am Armaturenbrett aufleuchtende rote Lampe «Warnung» bedeutet, er aber das Zeichen, welches sich unter der roten Lampe befindet und das den Ort des Problems angibt, nicht deuten kann, da es beispielsweise in chinesischer Sprache geschrieben ist. Sobald die Information dann aber verstanden wurde, verändert sich das Bewusstsein, da die Information entweder neu ist und der Kenntnisnehmer nun etwas mehr weiss als zuvor oder aber die Information sein schon vorhandenes Wissen bestätigt und dieses nun gefestigt wird.<sup>228</sup> Das Erfordernis des Verstehens hat zur Folge, dass selbst in Fällen, in denen Informationen auf ein Mitteilungshandeln der Person, über die sie etwas aussagen, zurückzuführen sind, sie erst mit den individuellen Prozessen beim Kenntnisnehmer vollendet werden und somit immer auf dessen Leistung angewiesen sind.<sup>229</sup> Damit ist aber auch gleich gesagt, dass dieselbe Information von verschiedenen Personen verschieden wahr- resp. aufgenommen werden kann, somit nicht bei jeder Person die gleiche Bedeutung, die gleiche Bewusstseinsveränderung hervorrufen muss.

#### 6.2.4 Definitionsversuch

Nehmen wir diese Unterscheidung zwischen dem abstrakten Etwas der Information als Inhalt und dem tatsächlich vermittelten Inhalt, dem Mehr an Wissen, zur Kenntnis, so ist Information zu definieren als *Möglichkeit der Bewusstseinsveränderung*. In diesem Sinne ist Information, solange sie noch nicht von einem Individuum wahrgenommen und für sich verstanden wurde, aussage-, gehalts- und bedeutungsneutral.<sup>230</sup> Information ist somit auch Information, wenn sie unwahr, unvollständig, ja vielleicht noch nicht einmal realisiert ist.<sup>231</sup> Auch die Grösse der Information ist nicht ausschlaggebend für deren Bestimmung als Information. So kann ein einzelnes Wort im selben Masse Information sein, wie ein ganzer Satz oder auch nur ein einzelner

---

<sup>228</sup> Vgl. GAUS, S. 31.

<sup>229</sup> ALBERS, Informationelle Selbstbestimmung, S. 131 f.

<sup>230</sup> Vgl. DRUEY, Information, S. 4.

<sup>231</sup> DRUEY, Information, S. 11.

## IV Kritik am herrschenden Verständnis und deren Würdigung

Buchstabe. Und auch die Art ihrer Erscheinung ist unbedeutend, kann sowohl ein Bild als auch ein geschriebener Text oder eine bloss gesprochene Mitteilung Information sein.

### 6.2.5 Fazit

Für die vorliegende Arbeit kann festgehalten werden, dass es sich bei Informationen um etwas Flüchtliges handelt, das die Möglichkeit der Bewusstseinsveränderung in sich trägt. Personeninformationen unterscheiden sich deshalb von den übrigen Sachinformationen nur aufgrund der Thematik, worüber sie eine Bewusstseinsweiterung hervorrufen können, nämlich über eine konkrete Person.

### 6.3 Was sind Daten?

Im Gegensatz zur Information sind Daten nichts Geistiges, sondern *Zeichen oder Zeichengebilde* (Buchstaben, Wörter, Zahlen, Symbole, etc.), die auf einem Datenträger (Papier, CD, etc.) *festgehalten* sind.<sup>232</sup> Daten sind etwas Festes, Beständiges mit der Folge, dass jeder, der das Datum sieht, dasselbe sieht. Allerdings bleiben nur die Daten beständig. Die aus ihnen herausgelesenen Informationen werden, wie vorne dargestellt, immer erst durch die interpretativen Leistungen des individuellen Kenntnisnehmers in der konkreten Situation erzeugt.<sup>233</sup> Daten alleine machen deshalb noch keine Information aus, sie müssen vielmehr aufgegriffen und über eine Deutungs- und Rekonstruktionsleistung verstanden werden.<sup>234</sup> Als Beispiel soll eine Blutanalyse dienen, die dem Arzt vom Labor nach der Untersuchung zugestellt wurde und welche er nun als Grundlage für seine Diagnose verwendet. Die einzelnen Blutwerte sind die Daten. Die konkrete Bedeutung, die der Arzt daraus entnimmt, also ob die einzelnen Werte dem Durchschnitt entsprechen oder ob sie Hinweise auf eine bestimmte Krankheit geben, ist sodann die Information, die der Arzt aufgrund seines Wissens daraus zieht. Ein anderer Arzt, der über mehr Fachwissen verfügt, zieht aus denselben Daten aber vielleicht eine ganz andere Information. Es kann so-

---

<sup>232</sup> ALBERS, Informationelle Selbstbestimmung, S. 89.

<sup>233</sup> Vgl. ALBERS, Informationelle Selbstbestimmung, S. 89.

<sup>234</sup> ALBERS, Informationelle Selbstbestimmung, S. 90.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

gar vorkommen, dass eine Person einem Datum eine Information entnehmen kann, eine andere jedoch nicht. So kann ein ausgebildeter Chemiker aus einer komplizierten chemischen Formel eine Information heraus ziehen, während diese für jemanden, der noch nie eine chemische Formel gesehen hat, keinen Sinn, also kein Mehr an Wissen, erzeugt, weil er einfach nichts damit anfangen kann. In diesem Sinne ALBERS: «Daten (können) syntaktisch dieselben Zeichen oder Zeichengebilde bleiben (...), während die an die Daten anknüpfenden Informationen erst mit der verstehenden Interpretation in der jeweiligen Situation erzeugt werden und einen variierenden Sinngehalt annehmen können.»<sup>235</sup> Mit Daten wird somit das Gefäß bezeichnet, in welches Informationen gekleidet werden, wenn sichergestellt werden soll, dass sie über einen unbegrenzten Zeitraum und für eine unbegrenzte Anzahl von potentiellen Kenntnisnehmern vorhanden bleiben. Ein Datum ist also immer das *Gefäß von Information*, ohne Information kein Datum. Dagegen ist das Datum keine Voraussetzung für die Information. Information kann auch nicht manifestiert sein, wenn sie beispielsweise mündlich weiter gegeben wird. Es könnte zwar argumentiert werden, dass auch die alleinige Übertragung per Schallwellen, ohne dass die Information noch auf andere Weise auf einem «festen» Träger festgehalten würde, eine Manifestation der Information darstellt und es sich deshalb bei rein akustisch wahrnehmbaren Informationen um Daten handelt. Dies geht der hier vertretenen Auffassung jedoch zu weit. Soweit Informationen nicht in einer Art festgehalten sind, dass jeder, der ohne Sehschwäche sehen kann, dasselbe sieht oder jeder, der die Information akustisch wahrnehmen kann, dasselbe wahrnimmt, und diese visuelle oder akustische Wahrnehmung nicht beliebig oft wiederholt werden kann, ohne dass sich etwas am Wahrgenommenen an und für sich ändert, handelt es sich um Informationen und nicht um Daten.<sup>236</sup>

---

<sup>235</sup> ALBERS, Informationelle Selbstbestimmung, S. 97.

<sup>236</sup> Es ist darauf hinzuweisen, dass das hier vorgestellte Verständnis von Informationen und Daten nicht zwingend mit jenem der Datenschutzgesetze übereinstimmen muss, da diese häufig das eine mit dem anderen zu erklären versuchen. So auch § 3 Abs. 3 IDG, der Personendaten als Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen definiert.

#### **6.4 Gibt es ein Selbstbestimmungsrecht bezüglich Informationen/Daten?**

Wie bereits vorne beim Thema Selbstbestimmung<sup>237</sup> erörtert, bedarf es dreier Voraussetzungen, um von Selbstbestimmung in einem gewissen Bereich zu sprechen: Freier Wille, eigene Handlung, die auf diesem freien Willen beruht, und, quasi als Grundvoraussetzung, die Möglichkeit, diese Handlung in der Realität auch umsetzen zu können – die Dispositionsfreiheit. Nachfolgend wird es darum gehen, das Vorhandensein dieser drei Voraussetzungen in Bezug auf Information und Daten zu überprüfen. Dabei wird der Fokus zuerst auf die Dispositionsfreiheit und erst dann auf den freien Willen und die eigene Handlung gelegt, da sich ohne ihre Bejahung die Überprüfung der weiteren Voraussetzungen erübrigt.

##### **6.4.1 Selbstbestimmung bezüglich Personeninformationen**

Bei der Frage nach der Selbstbestimmung bezüglich der die eigene Person betreffende Informationen muss unterschieden werden zwischen Informationen, die die betroffene Person selbst über sich hat, und Informationen, die andere Personen über die betroffene Person generieren. Denn wie ausführlich gezeigt wurde, handelt es sich bei Informationen um etwas Geistiges und in diesem Sinne um etwas Wandelbares. Eine Information ist nichts, das wir festhalten oder einschliessen können, sie existiert quasi im freien Raum und ist auf die individuellen Vorgänge des Wahrnehmens und Verstehens angewiesen. In diesem Sinne sind Informationen, auch wenn sie Aussagen über eine Person machen, nicht in einer Weise fassbar, als handle es sich um dieser Person anhaftende Eigenschaften, sondern sie bilden sich vorwiegend losgelöst von der Person, über die die Information etwas aussagen kann, im Bewusstsein anderer oder in Kommunikationszusammenhängen.<sup>238</sup> Dies verdeutlicht die Tatsache, dass Informationen ohne jedes Zutun der betroffenen Person gewonnen werden können, sei es durch Beobachtungen oder im Austausch mit anderen Menschen, was auch das Hörensagen und die freie Erfindung miteinschliesst.<sup>239</sup> In Bezug auf die *Dispositionsfreiheit* im Sinne von «im eigenen Einflussbereich liegend»

---

<sup>237</sup> Siehe Kapitel IV, Ziffer 6.1.

<sup>238</sup> ALBERS, Informationelle Selbstbestimmung, S. 88.

<sup>239</sup> ALBERS, Informationelle Selbstbestimmung, S. 89.



#### IV Kritik am herrschenden Verständnis und deren Würdigung

kann deshalb festgehalten werden, dass sich Informationen über die eigene Person sehr wohl im eigenen Einflussbereich befinden können, wenn eine Frau beispielsweise einen Schwangerschaftstest macht, dieser positiv ausfällt und sie keinem davon erzählt. In dem Moment, in dem die Frau diese Information jedoch mit anderen teilt, fließt die Information auch in den Einflussbereich anderer Personen. Die Information «Schwangerschaft» ist dann immer noch im Einflussbereich der Frau, aber eben nicht mehr exklusiv, wobei darauf hinzuweisen ist, dass die Exklusivität kein Wesensmerkmal der Dispositionsfreiheit im hier verstandenen Sinne ist, dies im Gegensatz zur sachenrechtlichen Verfügbarkeit. Informationen über die eigene Person – gleichgültig ob wahr oder falsch – von denen die betroffene Person keine Kenntnis hat, liegen jedoch ausserhalb des Einflussbereiches der betroffenen Person und eine Selbstbestimmung ist diesbezüglich rein faktisch nicht möglich. Die Dispositionsfreiheit kann somit nur für jene Informationen bejaht werden, in deren Kenntnis die betroffene Person ist, dies jedoch ohne die Ausschlussmöglichkeit anderer, die ebenfalls in Kenntnis dieser Information sind. Dementsprechend können auch nur für diese Informationen die weiteren Voraussetzungen der Selbstbestimmung – freier Wille und eine darauf beruhende Handlung – untersucht werden. *Freier Wille* erfordert die Wahl zwischen verschiedenen Möglichkeiten. Diese Wahl wird dann nicht mehr frei getroffen, wenn beispielsweise eine extreme seelische Belastung oder der Einfluss von bewusstseinsverändernden Substanzen die Sicht «vernebelt». Soweit sich die betroffene Person darüber hinaus auch nicht in einer Zwangssituation befindet, sind die dem freien Willen entsprechende Handlungen ebenfalls als frei zu verstehen, womit die Selbstbestimmung immerhin für jene Informationen, die sich im Einflussbereich der betroffenen Person befinden, bejaht werden kann.

##### **6.4.2 Selbstbestimmung bezüglich Personendaten**

Daten als Gefäss für Informationen sind im Vergleich zu Informationen grundsätzlich fassbar, und dies auch häufig im wahrsten Sinne des Wortes. Als Bild, Schriftstück oder Tonaufnahme sind sie dinglicher Natur. Sie können berührt, weggeschlossen, verschickt oder zerstört werden. Sobald solche *analoge Daten* aber in *digitale Daten* verwandelt werden – und das ist mit der heutigen Technik bei allen analogen Daten problemlos möglich, sind sie beliebig kopierbar und können grenzenlos weiterverarbeitet und verbreitet werden. Das Problematische daran ist, dass wenn die elektroni-

#### IV Kritik am herrschenden Verständnis und deren Würdigung

schen Daten erst einmal den Herrschaftsbereich einer Person verlassen haben (eigener PC, iPod, etc.), nicht mehr eruiert oder kontrolliert werden kann, ob die Daten verändert wurden und wer die Daten nutzt, weiterleitet etc. Immerhin kann gesagt werden, dass auch wenn andere über Daten zur eigenen Person disponieren, man selbst immer auch noch darüber disponieren kann, womit zumindest für jene Personendaten die *Dispositionsfreiheit* bejaht werden kann, welche sich (zumindest auch noch) im eigenen Herrschafts- resp. Kontrollbereich befinden. Anders ist die Sache zu beurteilen, wenn ein Datum Informationen zu einer Person wiedergeben kann, dieses sich aber nicht im Herrschaftsbereich der betroffenen Person befindet. Als Beispiel dient hier das Foto von der letzten Party, welches irgendjemand gemacht und ohne Kenntnis der Abgebildeten bei Facebook veröffentlicht hat. Die betroffene Person ist zwar auf dem Foto zu erkennen, es handelt sich also zweifellos um ein Datum zu ihrer Person. Da sie aber keine Kenntnis des Fotos hat und es sich so auch nicht zugänglich machen kann, liegt es ausserhalb ihres Einflussbereiches, womit die Dispositionsfreiheit für dieses Datum verneint werden muss.

Aufgrund der erörterten Unterscheidung zwischen Daten, die im eigenen Herrschaftsbereich liegen, und solchen, bei denen die betroffene Person keine Dispositionsmöglichkeit hat, muss auch in Bezug auf den freien Willen unterschieden werden. Ein *freier Wille* erfordert das Vorhandensein von Alternativen. Diese dürften bei einer Person in Bezug auf die sich in ihrem Herrschaftsbereich befindenden Daten vorhanden sein, kann sie diese geheim halten, weiter geben, zerstören, etc. Bezüglich derjenigen Daten, auf die sie keinen Einfluss ausüben kann, muss der freie Wille jedoch verneint werden, da die Person nicht bestimmen kann, wie damit umgegangen werden soll, womit ihr alternative Handlungsmöglichkeiten fehlen.

#### **6.5 Fazit**

Die vorangegangenen Darlegungen zeigen, dass das Grundrecht auf informationelle Selbstbestimmung auf sehr komplexen Erscheinungen fusst. Die Selbstbestimmung darf wohl als einer der in den menschlichen Köpfen am meisten verankerten Widersprüche bezeichnet werden. Denn obwohl wir davon ausgehen, dass wir autonom unsere Entscheidungen treffen, zeigen diverse Studien, dass dies gerade nicht der Fall ist und die uns so viel bedeutende Autonomie wohl öfters von unterbewussten

#### IV Kritik am herrschenden Verständnis und deren Würdigung

Mechanismen übersteuert wird. Gleichwohl ist unser Alltag, aber auch unser Rechtssystem, ganz selbstverständlich von der Idee geprägt, dass sich unsere Mitmenschen selbstbestimmt verhalten und nicht Werkzeug anderer oder ihres Unterbewusstseins sind.

Nicht weniger schwer zu fassen sind Daten und Informationen und deren Abgrenzung. Letztere ist zwar von einem gewissen dogmatischen Interesse, es muss allerdings bedacht werden, dass die noch zu erörternden Gefahren nicht durch die Daten und Informationen selbst entstehen, sondern durch den jeweiligen Umgang damit, was die Bedeutung der Abgrenzung ein wenig relativiert. Immerhin konnte für diese Arbeit festgehalten werden, dass es sich bei Informationen um flüchtige Sinngehalte handelt, die durch die interpretative Leistung einer Person zu einer Information für diese werden, während es sich bei Daten um manifestierte Informationen handelt, die damit letztlich unendlich vervielfältigbar und verteilbar werden. Die aufgeworfene Frage, ob Selbstbestimmung über solche Informationen und Daten möglich ist, musste kontrovers beantwortet werden. Selbstbestimmung in Bezug auf Informationen und Daten ist immerhin da möglich, wo sie sich im Einflussbereich der betroffenen Person befinden, für jene Informationen und Daten, die sich ausserhalb dieses Herrschaftsbereichs befinden, musste die Selbstbestimmung jedoch verneint werden, was die Existenzberechtigung eines Grundrechts auf informationelle Selbstbestimmung deutlich in Frage stellt.

## 7 Résumé und Überleitung

Die aufgezeigten Kritikpunkte machen deutlich, dass das herrschende Verständnis des Grundrechts auf informationelle Selbstbestimmung durchaus kritisch betrachtet werden muss. Gerade die Darlegung, dass Selbstbestimmung bezüglich die eigene Person betreffende Informationen und Daten nur in sehr eingeschränktem Masse möglich ist, stellt die Existenzberechtigung eines Grundrechts auf informationelle Selbstbestimmung deutlich in Frage. Im Folgenden soll deshalb untersucht werden, was aus Sicht des Rechts den Wert der Information ausmacht, welcher deren Schutz rechtfertigt?<sup>240</sup> Oder anders gefragt: Was setzen wir aufs Spiel, wenn wir die Exis-

---

<sup>240</sup> DRUEY, Information, S. 94.

#### IV Kritik am herrschenden Verständnis und deren Würdigung

tenzberechtigung des Grundrechts auf informationelle Selbstbestimmung verneinen und damit jedem das Recht einräumen, jederzeit Informationen und Daten über sich und alle anderen Personen, gegebenenfalls auch gegen deren Willen, zu beschaffen, zu verarbeiten, weiterzuleiten oder zu speichern?

## **V Schutzbedarfsanalyse**

### **1 Alltagssituationen und gesellschaftliche Konventionen**

Zu Beginn eine Alltagssituation: Ein Mann sitzt an seinem Schreibtisch und bohrt gedankenverloren tief in seiner Nase. Als er zum Eingang blickt, entdeckt er im Türrahmen seinen Kollegen, der ihn offenbar schon länger bei seiner Tätigkeit beobachtet. Sofort nimmt der Mann seinen Finger aus der Nase und schaut beschämt auf den Schreibtisch. Was ist geschehen? Das Bohren in der Nase ist weder für den Mann noch für seinen Arbeitskollegen schädlich, es ist ein notwendiges Übel, wenn etwas Störendes aus der Nase entfernt werden soll, und die meisten Menschen haben es schon mal getan. Wo liegt also das Problem? Das «Problem» besteht darin, dass das Nasenbohren in unserer Gesellschaft als «gruusig» und unhygienisch angesehen wird. Von Kindheit an wird uns beigebracht, dass man das nicht macht, und wenn man dann als Erwachsener bei einem derartigen *gesellschaftlichen Konventionsverstoss* erappt wird, fühlt man sich beschämt, in seinem Ansehen gemindert, denn man will ja nicht als «Grüsel» gelten. Dieses sehr einfache Beispiel soll zeigen, dass jeder Mensch, ob er dies nun möchte oder nicht, sehr stark von den Meinungen der Gesellschaft geprägt ist und sich im Normalfall darum bemüht, mit seinem Verhalten dieser Meinung zu entsprechen oder aber als Provokation sein Verhalten eben gerade entgegen den gesellschaftlichen Konventionen ausrichtet. Diese gesellschaftlichen Konventionen sind nun aber nicht zwingend identisch mit den eigentlichen Bedürfnissen der Individuen, weshalb es regelmässig zu Konventionsverstössen kommt. Dabei ist es für den einzelnen entscheidend, dass seine Verstösse geheim bleiben, denn nur so vermag er sein selbstgewähltes Ansehen in der Gesellschaft zu wahren.

### **2 Informationelle Privatheit und deren Verletzung**

RÖSSLER untersucht das beschriebene Phänomen unter dem Stichwort «informationelle Privatheit» und unterscheidet dabei grundsätzlich drei mögliche Arten von Verletzungen derselben: Die erste Variante ist der Fall des Voyeurs. Dabei wird eine

Person ohne ihr Wissen und gegen ihren Willen beobachtet. Beim zweiten Fall weiss die Person zwar, dass sie beobachtet wird oder dass Daten zu ihrer Person bearbeitet werden, dies geschieht jedoch gegen ihren Willen. Bei der dritten Variante weiss die Person wiederum um die Beobachtung, nimmt diese aber in Kauf, weil ihr andere Dinge, die sie dafür erhält, wichtiger sind.<sup>241</sup> Diese drei Fälle weisen allesamt Konstellationen auf, in denen es um den *Verlust der Kontrolle* sowie der Einschätzungsmöglichkeit darüber geht, was andere über die eigene Person wissen oder vor allem zu wissen glauben und als Informationen und/oder Daten an andere weitergeben. Aus der Ferne betrachtet könnte ein solcher Verlust als unerheblich gewertet werden, denn wenn eine Person beobachtet wird, andere Leute über sie sprechen oder wenn gar Daten über sie an andere Personen weiter gegeben werden, wird sie offenkundig nicht an irgendetwas gehindert, eine Einschränkung ihrer Freiheit ist prima facie nicht ersichtlich. Warum sollte eine Person also nicht mehr tun und lassen was sie will, nur weil andere sie dabei beobachten und diese Beobachtungen gegebenenfalls auf einem Datenträger speichern und einem unbegrenzten Publikum zugänglich machen, insbesondere dann, wenn sie von alledem gar nichts mitbekommt?<sup>242</sup>

### 3 Informationen und Daten prägen Rollen und Beziehungen

Die Bedeutung eines solchen Verlustes der Kontrolle und der Einschätzungsmöglichkeit über die Verwendung der eigenen Daten und Informationen sind eng mit den verschiedenen sozialen Rollen und Beziehungen verknüpft, die ein Mensch einnimmt und eingeht, und in der Art, wie er diese definiert und prägt. Jede Person lebt ihr Leben bewusst oder unbewusst, gewollt oder nicht, in unterschiedlichen sozialen Rollen und Beziehungen. Da gibt es die Rolle des Arbeiters, der Chefin, des Bürgers, der Steuerzahlerin, des Vaters, der Ehefrau, des Kumpels etc., die Beziehung zu den Eltern, Kinder, Lebenspartner, Arbeitskollegen, Nachbarn, Ärzten etc. Diese unterschiedlichen Rollen und Beziehungen definiert und reguliert der einzelne in erster Linie durch die Informationen, die er anderen über sich mitteilt und die Daten, die er

---

<sup>241</sup> RÖSSLER, S. 204.

<sup>242</sup> RÖSSLER, S. 206.

anderen über sich preisgibt oder eben nicht.<sup>243</sup> Beispiel: Eine Frau geht zum Arzt, um einen Aids-Test zu machen. In der Rolle als Patientin erzählt sie dem Arzt, dass sie in letzter Zeit mehrfach ungeschützten Geschlechtsverkehr gehabt hat. Im Rahmen der Beziehung zwischen ihr und dem Arzt erscheint ihr diese Information als angebracht. Als Abteilungsleiterin in einer grossen Firma, in der sie aufgrund des Firmenbildes für Werte wie Verantwortungsbewusstsein und soliden Lebenswandel einstehen muss, gibt sie die Informationen über ihr Sexualleben niemandem preis, denn diese könnten ihre Integrität als Vorgesetzte gefährden. Anderes Beispiel: Aufgrund eines akuten Erschöpfungszustandes verordnet der Arzt seinem Patienten ein teilweises Arbeitsverbot. Gegenüber seinen Fussballkumpels erwähnt der Patient jedoch nichts davon, aus Angst, sie würden ihn aufgrund dieser Kenntnis für einen Schwächling halten und die Beziehung zwischen ihnen würde darunter leiden. Die hier beschriebene *Selbstdarstellung* in den jeweils unterschiedlichen Rollen und Beziehungen darf nicht als theatralisches Sich-in-Szene-setzen-Wollen verstanden werden und hat auch nichts mit einem schauspielerischen Sich-Verstellen zu tun, bei dem der einzelne sein «wahres Ich» zu verbergen versuchte.<sup>244</sup> Im Gegenteil: Jede Rolle und Beziehung gehört zu diesem einen Ich, das in verschiedenen Lebensbereichen (Arbeitsplatz, Freunde, Familie, Militär etc.) mit unterschiedlichen Erwartungen konfrontiert wird oder seinen eigenen Erwartungen und Vorstellungen gerecht zu werden versucht.<sup>245</sup>

---

<sup>243</sup> RÖSSLER, S. 209; BULL, Informationelle Selbstbestimmung, S. 27; SCHWEIZER, S. 103; SCHAAR weist darauf hin, dass es gerade Eigenheit totalitärer Systeme sei, die private Sphäre einer vollständigen Kontrolle zu unterwerfen (SCHAAR, S. 19).

<sup>244</sup> DENNINGER, S. 112.

<sup>245</sup> So auch EVERS, demgemäss es zur freien Entfaltung der Persönlichkeit des einzelnen gehört zu bestimmen, «wie er in und zu der Umwelt stehen will und welches Persönlichkeitsbild die Umwelt von ihm haben soll. Ob sie von seinem Willen unabhängig ihr eigenes Urteil fällen wird, ist eine andere Frage. Der einzelne aber gibt ihr die Fakten für das Urteil». (EVERS, S. 39 f.); LUHMANN weist darauf hin, dass die Selbstidentifikation des Menschen als Vorgang zu begreifen ist, der sich im sozialen Kontakt vollzieht, also im Wissen darum, dass man mit jeder einsehbaren Lebensäusserung eine Aussage über sich selbst verbindet. Damit wird der Mensch die Persönlichkeit, als die er sich darstellt. (LUHMANN, S. 60); siehe zum These, dass es sich beim Menschen nicht um eine einschichtige Persönlichkeit handelt auch MÜLLER MARKUS, Selbstbestimmung, S. 69 (erörtert in Kapitel IV, Ziffer 6.1).

## 4 Enttäuschte Erwartungen

Damit der einzelne seine sozialen Rollen und Beziehungen frei, autonom und eigenverantwortlich definieren und regulieren kann, ist es aber von entscheidender Bedeutung, dass er weiss, mit wem er es zu tun hat, und er «von möglichst zutreffenden Informationen und Einschätzungen über den *Informations- und Wertungshorizont* seiner Interaktionspartner» ausgehen kann.<sup>246</sup> Denn nur wenn er ungefähr abschätzen kann, wer das Gegenüber ist und was es von ihm weiss, kann er sich darauf einstellen, wer er aufgrund dieses Wissens für den Anderen ist (in welcher Rolle oder Beziehung er sich gerade befindet), was aufgrund dessen von ihm erwartet wird und wie er sich selbst präsentieren muss, um dieser Rolle/Beziehung zu entsprechen und sie aufrecht zu erhalten.<sup>247</sup>

Dies kann auch bedeuten, dass die Erwartung einer Person diejenige ist, es mit keiner anderen Person zu tun zu haben, sie aber faktisch beobachtet wird, der Beobachter folglich mehr über sie weiss, als sie erwartet. Beispiel: Eine Frau ist alleine in ihrem Spitalzimmer, die Visite ist vorbei und sie fühlt sich völlig unbeobachtet. Sie stellt sich vor das Krankenbett und beginnt lauthals Arien von Verdi zu trällern und wild zu gestikulieren. Von der Dachterrasse gegenüber beobachten zwei Personen das ganze Theater.<sup>248</sup> Anderes Beispiel: Zwei Männer haben hinter der Hotelmauer Geschlechtsverkehr. Ein Hotelgast beobachtet die beiden und muss so laut lachen, dass die Männer realisieren, dass sie beobachtet wurden. Das Verhalten dieser Personen ist wesentlich von ihrer Erwartung bestimmt, dass niemand sie sieht und nie-

---

<sup>246</sup> DENNINGER, S. 112.

<sup>247</sup> RÖSSLER, S. 210 f.; STEINMÜLLER ET AL. haben dieses Phänomen in ihrem Gutachten anhand eines «kybernetischen Handlungsmodell» zu erläutern versucht: Jedes nach aussen tretendes Verhalten löse eine Reaktion der sozialen Umwelt aus, die darin bestehe, die im Verhalten enthaltenen Informationen über den Einzelnen zu rezipieren und gegebenenfalls mit weiteren schon bekannten Informationen zu einem Persönlichkeitsbild zu verarbeiten. Dieses Bild wirke wiederum auf den Einzelnen zurück, der es aufnehme und allenfalls sein künftiges Verhalten darauf ausrichte. Es sei mithin nicht gleichgültig, welche Informationen über den Einzelnen in seiner Umwelt bekannt seien, denn das Wissen der Umwelt stelle einen entscheidenden Faktor in der Persönlichkeitsentwicklung dar (STEINMÜLLER ET AL., S. 86 ff.). Ob das Gegenüber dem Einzelnen das präsentierte Bild seiner Selbst abnimmt, welches Bild sich das Gegenüber dann letztlich selbst von der Person macht und ob die Rechtsordnung das selbstgewählte Ansehen schützt und in welchem Rahmen sie dies tut, sind andere Fragen (siehe hierzu FN 245).

<sup>248</sup> Ausführliches Beispiel in BARTH, S. 70.



mand weiss, was sie gerade tun. Denn nur weil sie diese Erwartungen haben, verhalten sie sich genau so. Hätten sie von den Beobachtern gewusst, hätten sie sich mit aller Wahrscheinlichkeit anders verhalten.<sup>249</sup> Ohne diese Kenntnis war ihr Verhalten aber ein Verhalten unter *falschen Bedingungen*, ein nur scheinbar selbstbestimmtes Verhalten, scheinbar deshalb, weil die Annahmen, von denen die Frau und das Pärchen ausgegangen sind und auf deren Grundlage sie die Entscheidung für ihr jeweiliges Verhalten getroffen haben (Alleinsein, keiner kennt die Vorliebe für das Singen von Arien oder andere Männer) falsch waren.<sup>250</sup>

Werden die Erwartungen der betroffenen Person an ihr Umfeld und deren Wissen enttäuscht, indem jemand plötzlich etwas weiss oder zu wissen glaubt, das er aufgrund seiner Beziehung zu dieser Person, aus Sicht der letzteren, gar nicht wissen sollte, oder ist ohne Wissen des Betroffenen eine weitere Person involviert, erfolgt im Augenblick des Bewusstwerdens beim Getäuschten ein *Perspektivenwechsel*.<sup>251</sup> Dieser sieht sich nun so, wie ihn der Beobachter gesehen hat und gerade dieser Perspektivenwechsel verhindert laut RÖSSLER ein selbstbestimmtes Verhalten ohne Rücksicht auf andere oder nur auf solche, von deren Anwesenheit er weiss, denn auf einmal muss er die Tatsache berücksichtigen, dass er beobachtet wurde,<sup>252</sup> auf einmal sieht er sich so, wie ihn der andere gesehen, was aber nicht dem entspricht, wie er selbst gesehen werden wollte. BENN beschreibt dies wie folgt: «But if he stops merely because he's being watched, the interference is of quite a different kind. He could continue if he chose; being observed affects his action only by changing his own perception of it. The observer makes the action impossible only in the sense that the agent now sees it in a different light, through the eyes, as it were, of the observer (...).»<sup>253</sup> Die Aufrechterhaltung der ursprünglichen Rolle und Beziehung ist nach solch einer Interaktion nicht mehr möglich.<sup>254</sup> Durch das Mehr an Wissen der andern, welches eben nicht zur vor dem Vorfall bestehenden Rolle oder Beziehung passt, verändert sich die Rolle/Beziehung selbst und das gegen den Willen der betroffenen

---

<sup>249</sup> RÖSSLER, S. 207.

<sup>250</sup> RÖSSLER, S. 208.

<sup>251</sup> RÖSSLER, S. 210.

<sup>252</sup> RÖSSLER, S. 210.

<sup>253</sup> BENN, S. 272.

<sup>254</sup> Vgl. VON INS/WYDER, BaKomm StGB, N 24 f. zu Art. 179<sup>bis</sup> StGB.

Person. Beispiel: Der Arbeitgeber einer psychisch angeschlagenen Frau erfährt per Zufall, dass sie Psychopharmaka einnimmt. Vom Moment der Kenntnisaufnahme ihrer Krankheit an überlegt er sich täglich, ob er ihr eine Aufgabe zumuten kann oder nicht. Die Frau bemerkt die Veränderung, weiss aber nicht, was geschehen ist, und verhält sich deshalb zunehmend zurückhaltend. Dies wertet der Arbeitgeber wiederum als Zeichen der Überforderung. Dieses Beispiel macht verständlich, weshalb es für die Beurteilung des Schutzbedarfs bezüglich der Selbstbestimmung über die eigene Person betreffenden Informationen und Daten keine Rolle spielt, ob die betroffene Person erfährt, dass sie beobachtet wird oder dass Informationen über sie ausgetauscht wurden oder nicht. Denn ihr Verhalten ist in jedem Fall ein Verhalten unter falschen Voraussetzungen, ein nur *vermeintlich selbstbestimmtes Verhalten*, da eine andere Person etwas über sie weiss, von dem sie nicht weiss, dass diese Person besagte Kenntnis hat.

## 5 Die Konsequenzen

### 5.1 *Angepasstes Verhalten*

Muss eine Person nun ständig davon ausgehen, dass andere Leute mehr von ihr wissen, als sie aufgrund der von ihr verbreiteten Informationen wissen sollten, dann ist ihr Verhalten eben darauf gerichtet, das heisst sie passt sich an.<sup>255</sup> Müsste die im Spitalzimmer ariensingende Frau davon ausgehen, dass sie jederzeit beobachtet werden könnte, würde sie ihr Verhalten mit aller Wahrscheinlichkeit anpassen und Singen und Gestikulieren gänzlich einstellen. Dieses Verhalten wäre mangels echter Alternativen aber nicht selbstbestimmt.<sup>256</sup> Die Frau gäbe sich nicht mehr so, wie sie eigentlich gerne wäre, sondern sie passt sich an und verstellt ihr eigentliches Verhalten, weil sie davon ausgeht, dass die Kenntnis ihrer Vorlieben sie bei anderen Personen in ein nicht von ihr gewolltes Licht setzen würde. Das selbe gilt für die beiden homosexuellen Hotelgäste. Wären sie davon ausgegangen, dass sie beim Ge-

---

<sup>255</sup> Dies hat auch das Bundesgericht so gesehen, als es in BGE 113 Ia 1 ff. (6), E. 4b konstatierte, dass ein Registereintrag die betroffene Person allenfalls davon abhalten kann, sich völlig frei zu bewegen.

<sup>256</sup> Zu den allgemeinen Voraussetzungen für die Selbstbestimmung siehe Kapitel IV, Ziffer 6.1.

schlechtsverkehr beobachtet werden, hätten sie sich aller Wahrscheinlichkeit nach anders verhalten.<sup>257</sup>

### 5.2 *Steigende Tendenz bei Manifestation*

Die Tendenz, sich ungeachtet der eigenen Bedürfnisse und Überzeugungen anzupassen, nimmt zu, wenn damit gerechnet werden muss, dass das Beobachtete nicht einfach als Information bei den Beobachtern bleibt, sondern als Daten festgehalten wird, die jederzeit einer unbestimmten Anzahl von Personen über einen unbestimmten Zeitraum hinweg zugänglich gemacht werden können. Denn durch die *Beständigkeit des Datums* ist ein Leugnen oder die Wiedergabe der Situation in eigenen Worten oder aufgrund der eigenen Interpretation kaum mehr möglich.<sup>258</sup> Dies stellen aber gerade solche Handlungen dar, die dazu dienen, das Bild, das wir von uns selbst abgeben möchten, möglichst aufrechtzuerhalten (oder zumindest mitzubestimmen), um so unsere Beziehungen und Rollen bewahren zu können.<sup>259</sup> Und gerade diese Mechanismen sind es, die als Grundlage für die weit verbreiteten und noch weiter geforderten Videoüberwachungen dienen. Ungeachtet der Frage, ob solche Systeme tatsächlich zielführend sind oder ob sie das Problem nur verlagern, ist doch zu beobachten, dass die Mehrheit der Leute in solch überwachten Zonen versucht, sich (rechts- und sozial)konform zu verhalten, sofern die Überwachung bekannt ist.<sup>260</sup>

Es ist aber nicht nur die Beständigkeit eines Datums alleine, welche sich negativ auf die betroffene Person auswirkt, auch wenn dies für WARREN/BRANDEIS noch so ge-

---

<sup>257</sup> In die selbe Richtung geht das zu beobachtende Verhalten von Menschen, welche in einem modernen Wohnanlage mit vielen Fenstern wohnen. Die meisten Mieter richten nicht etwa das Schlafzimmer in diesen einsehbaren Räumen ein, sondern ihre Küche oder das Wohnzimmer. Und selbst diese Räume werden gerne mit Rollos oder Vorhängen oder ganz vielen grossen Pflanzen von der Aussenwelt abgeschirmt.

<sup>258</sup> Im Google-Street-View-Entscheid hat das Bundesgericht anerkannt, dass die Befürchtung von Betroffenen, dass aus den Aufzeichnungen falsche oder sie persönlich belastende Schlüsse gezogen werden könnten, nicht von der Hand zu weisen sei (BGE 138 II 346 ff. (361), E. 8.3).

<sup>259</sup> Zur Beeinflussung des eigenen Bildes siehe FN 244.

<sup>260</sup> Vgl. zum Ganzen: JEAN BUSCHÉ, *Vidéosurveillance: mise en perspective du cas genevois et point de vue éthique*, Genf 2013.

wesen sein mochte.<sup>261</sup> Wirklich problematisch erscheinen die *unbeschränkte Verteilbarkeit* und die *endlose Speicherung* eines Datums. Obwohl früher schon die Möglichkeit bestand, ein analoges Datum durch Kopieren zu vervielfältigen, waren dessen Verteilbarkeit aufgrund der damit zusammenhängenden Kosten, aber auch aufgrund der dafür aufzuwendenden Zeit, Grenzen gesetzt. Hinzu kam, dass durch den begrenzt vorhandenen Speicherplatz nicht jedes Datum aufbewahrt wurde, sondern eine Reduktion auf das Wesentliche stattfinden musste, dieser Speicherplatz ebenfalls Kosten verursachte und das Wiederfinden eines bestimmten Datums per Handgriff doch eher mühselig und zeitintensiv war. Durch die Digitalisierung, die technischen Errungenschaften bezüglich Speicherkapazität und die Erfindung des Internets haben sich die Vorzeichen jedoch markant geändert, und so ist es heute möglich, in kürzester Zeit eine riesige Menge von Daten jeder Person mit Internetzugang zugänglich zu machen, sie abzuspeichern, per Mausklick wieder darauf zuzugreifen und all dies zu minimalen Kosten. Beispiel: Der beobachtende Hotelgast stellt sein Filmchen über die beiden Männer beim Geschlechtsakt ins Internet. Menschen aus dem Bekanntenkreis des einen Mannes entdecken das Filmchen und schicken es seiner Frau, die weder Kenntnis von der Homosexualität ihres Ehegatten hatte noch von seinem derzeitigen Urlaub. Die Frau reicht daraufhin die Scheidung ein. Der Arbeitgeber des Mannes, ein katholischer Geistlicher, dem die Frau alles erzählt hat, kündigt ihm. Wäre der Film vor dreissig Jahren auf VHS aufgezeichnet worden, wäre das Doppelleben des Mannes wohl nicht aufgedeckt worden, da es doch eher unwahrscheinlich erscheint, dass der Filmemacher den Film so oft kopiert und per Post an genau die Leute verschickt hätte, die den Mann kennen.

Das Problematische an diesen neueren Möglichkeiten, beliebige Daten über beliebige Personen zu erhalten, weiterzuleiten, zu speichern etc. ist, dass ein Vergessenwerden nahezu komplett verunmöglicht wird.<sup>262</sup> Ohne die Möglichkeit des *Vergessenwerdens* nehmen wir uns aber zumindest langfristig die Möglichkeit, uns so zu verhalten, wie es unseren eigenen Ideen entspricht, da wir ständig damit rechnen müssen, mit unserem heutigen Verhalten auch in zwanzig, dreissig oder vierzig Jah-

---

<sup>261</sup> Vgl. WARREN/BRANDEIS, S. 193 ff.

<sup>262</sup> Siehe SCHERTZ/HÖCH, S. 195.

ren konfrontiert zu werden.<sup>263</sup> Auch BELSER anerkennt, dass Datenbearbeitungen die freie Urteils- und Entscheidungsbildung eines einzelnen erheblich stören und dadurch sogar seine Würde gefährden können, etwa durch das Gefühl des ständigen Überwachtseins, den Verlust einer abgeschirmten Privatsphäre oder durch das Bewusstsein, dass jede Handlung oder Meinungsäußerung beliebig lang registriert wird und es kein Recht auf Fehler, Veränderung und Vergessen gibt.<sup>264</sup>

Hinzu kommt, dass durch die Informationsallokation im Netz und die damit zusammenhängenden Informationsverschiebungen *Machtverschiebungen* entstehen können. Wer in «Besitz» von Daten zu einer anderen Person ist, von denen er weiss, dass die sich daraus ergebenden Informationen nicht in die jeweiligen Beziehungen passt (er also jene Daten auch gar nicht besitzen dürfte), kann diese gegen den Betroffenen spielen lassen, ihn also erpressen und somit Einfluss auf seine Handlungen ausüben. Dies gilt selbstredend nicht nur für Daten im World Wide Web, aber gerade durch dessen «ewiges Gedächtnis» verliert der Mensch sein natürliches «Recht» auf Rehabilitation, denn er wird zum durchschaubaren Objekt und als solches beeinflussbar. So weist auch RUDIN darauf hin, dass ein *gläserner Mensch* ein *manipulierbarer Mensch* ist.<sup>265</sup> BURKERT hebt das Ganze auf eine andere Ebene, indem er darauf aufmerksam macht, dass Informationsasymmetrien Ausdruck von Machtverteilungen sind und Machtverteilungen gesellschaftliche Steuerung und Entwicklung ermöglichen.<sup>266</sup> Die informationelle Selbstbestimmung dient eben nicht nur dem Individuum. Wie noch zu zeigen sein wird, ist sie vielmehr auch als elementare Voraussetzung für das Funktionieren einer Gesellschaft und damit des Staates und der Wirtschaft zu verstehen.<sup>267</sup>

---

<sup>263</sup> Siehe <<http://www.edoeb.admin.ch/datenschutz/00683/01173/index.html?lang=de>> (zuletzt besucht am 23.9.2014).

<sup>264</sup> BELSER, Instrumente, S. 30; vgl. auch WOLLENTEIT, S. 248 oder SAINT-MONT, S. 96.

<sup>265</sup> RUDIN, Datenschutzaufsicht, S. 410; vgl. auch KARG, S. 76.

<sup>266</sup> BURKERT, S. 16.

<sup>267</sup> RUDIN, Datenschutzaufsicht, S. 410 f.; KARG, S. 76 f.

## 6 Private «Räume» als essentielle Voraussetzung

Unabhängig von der Frage, welches Verhalten als moralisch richtig oder falsch zu werten ist, deren Beantwortung im Übrigen je nach Ort, Zeit und Raum verschieden ausfällt, ist es für die Entwicklung des Menschen zentral, gar entscheidend, dass es Räume i.S.v. Momenten, Sphären, Orte gibt, die dem Zugang anderer ohne Einwilligung des Betroffenen verwehrt sind, und dass Daten, welche Situationen in solchen Räumen wiedergeben, nur mit dem Einverständnis des Betroffenen generiert und weiterverarbeitet oder weiterverbreitet werden.<sup>268</sup> Nur wenn solche «Räume» existieren dürfen und dem einzelnen das Recht zukommt, sich diese Räume zu schaffen und zu bewahren, indem er über den Umgang mit den Daten zu seiner Person aus diesen «Räumen» bestimmen kann, kann sich ein Individuum, gedacht mit all seinen ihm eigenen Fehlern und Talenten, erleben, sich dadurch kennen lernen, Vertrauen in das eigene Selbst gewinnen und sich somit letztlich zu einer selbständigen und eigenverantwortlichen Person entwickeln.<sup>269</sup> Es geht eben nicht darum – wie gerne etwas lapidar angenommen wird – ob man etwas zu verbergen habe oder eben nicht, sondern es geht um die Grundvoraussetzung zur Entwicklung von *autonomen Personen*.<sup>270</sup>

Und gerade diese autonomen Personen sind es, die das *Fundament* einer Demokratie und des friedvollen menschlichen Zusammenlebens schlechthin bilden.<sup>271</sup> Denn auch wenn, wie bereits an anderer Stelle erwähnt,<sup>272</sup> das Ideal eines autonomen

---

<sup>268</sup> Gleicher Meinung SCHWARZ, S. 15; vgl. auch VON INS/WYDER, BaKomm StGB, N 8 zu Art. 179<sup>quater</sup> StGB.

<sup>269</sup> Vgl. SCHERTZ/HÖCH, S. 23; vgl. auch EVERS, S. 39 f.

<sup>270</sup> Vgl. SCHERTZ/HÖCH, S. 34; es wäre deshalb auch sehr naiv davon auszugehen, dass sich nur jener bedroht fühlen muss, der etwas zu verbergen hat. Zu verbergen haben wir alle etwas, oder mit den Worten von BULL: «(...) die Behauptung, man habe vor den Behörden oder den Mitmenschen nichts zu verheimlichen, widerspricht allen Erfahrungen des Alltagslebens. Da will doch jeder nur das über sich, seine Familie, seinen Beruf und seine Geschäfte verbreiten, was ihm vorteilhaft erscheint, und selbst derjenige, der sich gern selbst ironisiert oder aus öffentlicher Selbstkritik Befriedigung gewinnt, vermeidet es im Allgemeinen, sich ernststen Gefahren auszusetzen. Wer wird schon ohne Not behaupten, gegen das Strafgesetz verstossen zu haben? Wer wird durch unnötiges Offenbaren wirtschaftlicher Bedrängnis seinen Kredit gefährden?» (BULL, Datenschutz, S. 11).

<sup>271</sup> SCHWARZ, S. 12.

<sup>272</sup> Siehe Kapitel IV, Ziffer 6.1.

Menschen vielleicht nicht immer oder ganz der Realität entspricht, so baut unsere Gesellschaft, unser Wert- und damit unser Rechtssystem, doch unmittelbar darauf auf. Alle Menschen, zu denen wir Beziehungen in irgendeiner Art pflegen, gehen letztlich davon aus, dass wir unsere Entscheidungen aufgrund unserer eigenen Gedanken und Meinungen treffen und nicht bloss das willenlose Werkzeug eines anderen darstellen. Denn wenn wir dauernd davon ausgehen müssten, dass andere Menschen fremdbestimmt werden, zumindest in dem Sinne, dass sie sich an irgendwelche Anforderungen anpassen aus Angst, sonst mit Repressionen irgendwelcher Art rechnen zu müssen, würden wir keine Beziehungen zu diesen anderen eingehen, wir würden nicht vertrauen, und wir wären nicht in der Lage, weder als Privatperson noch als Bürger, Entscheidungen für uns zu treffen, die auch tatsächlich unseren Bedürfnissen, Überzeugungen und Wünschen entsprechen.<sup>273</sup> In ähnlicher Weise argumentierte auch das Bundesverfassungsgericht im Volkszählungsurteil: «Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8 f. GG) verzichten. Dies würde nicht nur die *individuellen Entfaltungschancen* des einzelnen beeinträchtigen, sondern auch das *Gemeinwohl*, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.»<sup>274</sup> Ja auch eine auf Wettbewerb basierende *Wirtschaft* kann nicht von manipulierbaren Konsumenten profitieren, da Manipulation den Wettbewerb verfälscht.<sup>275</sup>

Hieraus folgt, dass eine freie Persönlichkeitsentfaltung unter den modernen Bedingungen der Datenverarbeitung den Schutz des Individuums vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus-

---

<sup>273</sup> Vgl. RÖSSLER, S. 218.

<sup>274</sup> BVerfGE 65, 1 (46).

<sup>275</sup> RUDIN, Datenschutzaufsicht, S. 410.

setzt.<sup>276</sup> Oder mit den Worten von RÖSSLER: «Ohne die selbstbestimmte Kontrolle darüber, wem man was über sich erzählt und wie man sich somit selbst präsentiert, ist die selbst gewählte Unterschiedlichkeit von Beziehungen aber nicht möglich und damit auch nicht das selbstbestimmte kontextuell je unterschiedliche authentische Verhalten anderen gegenüber und damit nicht die unterschiedlichen, selbst gewählten Formen der Auseinandersetzung mit anderen.»<sup>277</sup> Somit kann gesagt werden, dass individuelle Autonomie auf informationelle Privatheit angewiesen ist,<sup>278</sup> und diese wiederum nur durch die Entscheidungsfreiheit über die persönlichen Kommunikationsbeziehungen, über das von der Rechtsordnung zugestandene Dispositionsrecht über die Informationen und Daten zur eigenen Person, gewährleistet werden kann.<sup>279</sup>

## **7 Informationen und Daten brauchen keine Relation in der Realität**

Die gemachten Ausführungen bezüglich der negativen Konsequenzen einer verlorengegangenen oder inexistenten Einflussmöglichkeit über die die eigene Person betreffenden Daten und Informationen wiegen umso schwerer, als solche Daten und Informationen keinen real bestehenden Konnex zur betroffenen Person aufweisen müssen, sondern *frei erfunden* oder von fremder «Hand» *neu generiert* sein können.

Bei ersterem Phänomen ist vor allem an Fotomanipulationen per Computerprogramm oder an das Streuen von Gerüchten zu denken. Solche Szenarien dürften sich wohl vor allem im Kontext persönlicher Beziehungen zwischen Betroffenen und Daten-/Informationserfinder abspielen, wobei virtuelle Kontakte genügen, und betreffen normalerweise eine bestimmte Anzahl Personen.

---

<sup>276</sup> BVerfGE 65, 1 (46).

<sup>277</sup> RÖSSLER, S. 209.

<sup>278</sup> RÖSSLER, S. 203.

<sup>279</sup> SCHWEIZER, S. 103; dies schliesst jedoch nicht aus, dass der Umgang mit solchen Informationen und Daten ausschliesslich den Betroffenen zusteht. Der Gesetzgeber kann freilich vorsehen, dass der Umgang mit personenbezogenen Daten und Informationen auch gegen den Willen der betroffenen Personen zulässig ist, sofern er dabei das Grundrecht nicht aushöhlt (siehe dazu Kapitel IV, Ziffer 3). Darüber hinaus kann dem Menschen auch nicht verwehrt werden, sich eine Meinung über eine Person zu bilden, die ggf. nicht mit deren Wunschbild von sich übereinstimmt (siehe FN 244).



Das zweite Phänomen fungiert unter dem Begriff «*big data*» und es ermöglicht durch die Speicherung und Verknüpfung riesiger Datenmengen das Entstehen von neuen Daten, welche neue Informationen über eine bestimmte Person hervorbringen können.<sup>280</sup> Dabei müssen die zusammengeführten Daten weder besonders genau sein, noch einen eigentlichen Personenbezug aufweisen. Je grösser die Datenmenge, desto mehr steigt die Wahrscheinlichkeit, dass die daraus gewonnen Daten wieder bestimmten Personen zugeordnet werden können.<sup>281</sup> Studien haben gezeigt, dass lediglich drei demografische Merkmale wie Geschlecht, 5-stellige Postleitzahl und volles Geburtsdatum reichen, um zwischen 61 bis 87 % der amerikanischen Bevölkerung eindeutig identifizieren zu können.<sup>282</sup> Das Ziel dieser «*big data*»-Technologien ist es, in noch nie dagewesener Genauigkeit Daten über alle möglichen Personen zu sammeln und durch deren Analyse die Realität mehr oder weniger zuverlässig abzubilden, ja sogar *vorherzusagen*, grundsätzlich um den Unternehmen zu ermöglichen, ihr Sortiment optimal an den Kunden anzupassen.<sup>283</sup> Solche erfundenen oder berechneten Daten und Informationen bergen aber gerade aufgrund ihrer nicht vorhandenen Relation zur faktischen Realität eine besondere Gefahr für die Betroffenen, sobald sie den Eindruck zu erwecken vermögen, richtig zu sein. Sie geben ein Bild dieser Person ab, das diese nicht nur nicht selbst gewählt hat, sondern das nicht Inhalt irgendeines ihrer Teilchens ist oder höchstens in sehr verzerrter oder verkürzter Weise. Die betroffene Person wird von anderen aufgrund dieser unrichtigen oder unvollständigen Informationen und Daten nicht korrekt eingeschätzt. Anders als bei der Auseinandersetzung mit dem Umstand, dass andere mehr zur eigenen Person wissen, als sie dies aufgrund der bestehenden Beziehung tun sollten, muss sich die betroffene Person bei erfundenen Daten und Informationen etwas anrechnen lassen, was faktisch nicht zu ihrer Person gehört. Die Problematik ist hier ähnlich jener bei der *üblen Nachrede* oder *Verleumdung* nach Art. 173 f. StGB und kann sogar in einer solchen enden: Durch eine Handlung tritt eine Veränderung der Bewertung der be-

---

<sup>280</sup> Vgl. BONDOLFI, S. 134.

<sup>281</sup> BAERISWYL, «Big Data», S. 15.

<sup>282</sup> KARJOTH, S. 19 mit Verweis auf die Studien von SWEENEY und GOLLE.

<sup>283</sup> Vgl. POLZER, S. 7 ff.

troffenen Person durch ihre Mitmenschen zu ihren Ungunsten ein,<sup>284</sup> und dadurch stehen die davon betroffenen Rollen und Beziehungen unter falschen Voraussetzungen.<sup>285</sup> Bei berechneten Daten können diese sehr wohl «richtige» Aussagen über die betroffene Person treffen, jedoch völlig von der eigentlichen Person isoliert.<sup>286</sup> Denn mit den «big data»-Technologien können wir zwar das «Was» analysieren, jedoch nicht das «Warum», und aus den Vorhersagen werden Schuldvermutungen, Schuldzuschreibungen oder gar Strafen abgeleitet.<sup>287</sup> So setzt beispielsweise die Polizei in Memphis ein Datenanalyseprogramm namens «Blue CRUSH» ein, welches aufgrund eines Algorithmus helfen soll, Strassen, Gruppen, sogar einzelne Personen zu identifizieren, welche stärker überwacht werden sollen, da sie laut System anfälliger für bestimmte Verbrechen sind.<sup>288</sup> Beim Forschungsprojekt «FAST» wird im Auftrag des Heimatschutzministeriums der USA versucht, allfällige Terroristen auszumachen, indem es spezifische physiologische Faktoren überprüft. Im Gegensatz zu der sich schon lange im Einsatz befindenden Methode des Profiling, bei der man eine Gruppe von Menschen, die alle ein gemeinsames Merkmal aufweisen, einer Regel unterwirft, also Mann – arabische Abstammung – oneway-Ticket = Terrorist, geht es bei «big data»-Analysen nicht um Pauschalverdächtigungen durch Gruppenzugehörigkeit, sondern man versucht, auf den einzelnen abzielen.<sup>289</sup> Das offensichtlich Problematische an solchen Verfahren ist, dass dadurch Menschen für ihr Verhalten zur Verantwortung gezogen werden, obwohl sie sich noch gar nicht so verhalten haben, also durchaus die Möglichkeit besteht, dass sich diese Menschen tatsächlich anders verhalten werden. Dies betrifft nebst der erwähnten Strafverfolgung auch Entscheidungen von Unternehmen, ihren Mitarbeitenden beispielsweise aufgrund eines er-

---

<sup>284</sup> RIKLIN, BaKomm StGB, N 12 zu Vor Art. 173.

<sup>285</sup> Als Beispiel für die möglichen gravierenden Folgen solch erfundener Daten kann der Fall eines 17-jährigen Jugendlichen genannt werden, der nach einer Hetzkampagne auf der Internetseite «isharegossip.com» von 20 anderen Jugendlichen bis zur Bewusstlosigkeit zusammen geschlagen wurde, weil er seine Freundin vor dem Internet-Mobbing der Mitschülerinnen in Schutz nehmen wollte, gefunden auf: <<http://www.welt.de/vermischtes/weltgeschehen/article12923939/Brutale-Attacke-auf-17Jaehrigen-entsetzt-Berlin.html>> (zuletzt besucht am 17.11.2014).

<sup>286</sup> Vgl. <<http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/big-data-studie-wir-verlieren-die-hoheit-ueber-unsere-daten-12831709-p2.html>> (zuletzt besucht am: 3.10.2014).

<sup>287</sup> Interview mit Viktor Mayer-Schönenberger auf <<http://www.srf.ch/news/panorama/big-data-die-vorteile-ueberwiegen-die-gefahren>> (zuletzt besucht am: 3.10.2014).

<sup>288</sup> MAYER-SCHÖNBERGER/CUKIER, S. 200.

<sup>289</sup> MAYER-SCHÖNBERGER/CUKIER, S. 202.

warteten Verhaltens zu künden, oder die Entscheidung eines Spitals, einem Patienten die notwendige Behandlung zu verweigern, weil man davon ausgeht, dass er den Behandlungserfolg mit seinem künftigen Verhalten sabotieren wird und so die Behandlung nicht verdient habe. Eine auf einem solchen System aufbauende Gesellschaft führt jedoch zu «Kollektivierung unserer Entscheidungsfreiheit» und damit zur Vernichtung des freien Willens.<sup>290</sup>

## 8 Nicht jede Information, jedes Personendatum schützenswert?

### 8.1 Kategorisierung von Daten

Gerade das eben beschriebene «big-data»-Phänomen zeigt, dass jedes Personendatum, jede Information zu einer Person im Grossen und Ganzen Relevanz besitzt. Verschiedene Autoren gehen jedoch davon aus, dass nicht jede Information oder jedes Datum zu einer Person per se schützenswert ist. So ist BELSER der Ansicht, dass es belanglose Informationen gebe, deren Schutzwürdigkeit zu verneinen sei<sup>291</sup> und nach VOGELSANG gibt es so etwas wie «Bagatelldaten», welche nicht unter den Schutzbereich der informationellen Selbstbestimmung fallen.<sup>292</sup> DRUEY spricht von einer in unserer Zeit festzustellenden Tendenz, den Schutz auf Intimdaten zu beschränken.<sup>293</sup> Es mag auf den ersten Blick einzusehen sein, dass nicht jedes Datum, welches einen Personenbezug aufweist, schützenswert erscheint, denn es ist nicht leicht einzusehen, was es beispielsweise an einer Adresse zu schützen gilt oder an der in einer Krankengeschichte festgehaltenen Diagnose, dass eine Frau schwanger ist. Diese Ansicht geht jedoch fälschlicherweise davon aus, dass Personendaten kategorisiert werden könnten in sensitive Daten, die es per se zu schützen gelte, und solche, die eben per se keines Schutzes würdig sind. Es mag wohl sein, dass gewisse Daten grundsätzlich ein höheres *Gefährdungspotential* aufweisen als andere, weil sie häufig einen Stigmatisierungseffekt haben, wie beispielsweise eine gesundheitliche Prädisposition oder eine Religion. Deshalb verlangen die Datenschutzgesetze

---

<sup>290</sup> MAYER-SCHÖNBERGER/CUKIER, S. 204 f.; siehe zum Ganzen WERNER, S. 54 ff.

<sup>291</sup> Vgl. BELSER, Instrumente, S. 27.

<sup>292</sup> VOGELSANG, S. 61 f.

<sup>293</sup> DRUEY, Strukturelle Schwäche, S. 147.

für solche Daten auch höhere Hürden bei deren Bearbeitung. Verallgemeinert auf alle Daten gilt dies jedoch nicht, denn es kommt entscheidend auf den Verwendungszweck der Personendaten an.<sup>294</sup>

Je nach Kontext wird ein an und für sich belangloses Personendatum zu einem sehr sensitiven, weil der Kontext das Gefährdungspotential erhöht.<sup>295</sup> So wird die Adresse in einem Zeugenschutzprogramm auf einmal zu einem höchst schützenswerten Datum, und die in der Krankengeschichte festgehaltene Information, dass eine Frau schwanger ist, führt in den Händen ihres potentiellen neuen Arbeitgebers dazu, dass sie die Stelle doch nicht erhält.

### 8.2 5-Elemente-These

Nach MAYER-SCHÖNBERGER hängt die Anerkennung eines subjektiven Rechts an Information von der *Beziehungsintensität* der Subjekt-Objekt-Relation ab: Erst wenn sich die durch die Intensität der Relation vom Individuum zur Information zu einer der Sachherrschaft ähnlichen Verfügungsgewalt entwickelt habe und sich von der Information zurück zum Individuum zu einem relevanten Mosaikstein seiner Identität und Persönlichkeit verdichtet habe, greife der grundrechtliche Schutz und konstituiere sich zum subjektiven Recht.<sup>296</sup> Das Vorliegen eines subjektiven Rechts hänge also von einzelnen Elementen ab, wobei das erste Element der Indikator für die *Nachhaltigkeit* des Vorhandenseins einer Information sei. Dieses Mass an «Manifestation» von Information liege umso stärker vor, je weniger flüchtig, je permanenter und offenkundiger die Information sei.<sup>297</sup> Als zweites Element bezeichnet er das Mass für die *Zuordnungsnähe* einer Information zu einem bestimmten Objekt. Je offensichtlicher eine Information einem bestimmten Subjekt zugeordnet werden könne, desto wahrscheinlicher ist der Schutz dieser Relation durch ein subjektives Recht. Als Drit-

---

<sup>294</sup> Siehe auch SIMITIS, Kommentar BDSG, N 251 zu § 3 BDSG.

<sup>295</sup> Dies darf nach ALBERS jedoch nicht dahingehend verstanden werden, dass der Verwendungskontext Umfang und Intensität des rechtlichen Schutzes bestimme. Der Schutz richte sich nicht nach dem Verwendungszusammenhang, sondern nach der Grundrechtsnorm (ALBERS, Informationelle Selbstbestimmung, S. 161 f.).

<sup>296</sup> MAYER-SCHÖNBERGER, S. 58.

<sup>297</sup> Zur Manifestation von Informationen siehe Kapitel IV, Ziffer 6.3.

tes sei die Stärke der *persönlichkeitstangierenden Dimension* der Information zu prüfen. Je intensiver eine Information die Persönlichkeit des ihm zugeordneten Subjekts betreffe, desto stärker sei die Subjekt-Objekt-Relation zwischen Information und Subjekt. Das vierte von MAYER-SCHÖNBERGER genannte Element ist ein Mass für die *Marktfähigkeit* der Information. Je «kommodifizierbarer», sprich marktfähiger eine Information sei, desto stärker werde das Bedürfnis des Subjekts in der Subjekt-Objekt-Relation sein, über die ihm zugeordnete Information disponieren zu können. Das fünfte Element bestimme sodann, in welchem Mass auch juristische Personen im konkreten Fall «*Persönlichkeit*» besitzen und damit gegebenenfalls Subjekte in eine informationsrechtlichen Subjekt-Objekt-Relation sein können.<sup>298</sup> Die von MAYER-SCHÖNBERGER entwickelte Theorie, dass nur bestimmte Daten schützenswert sind und sich diese Schutzwürdigkeit anhand seiner 5-Elemente-These eruieren lasse, verliert nach einer möglichst klaren Differenzierungen zwischen Daten und Informationen sowie Daten und Personendaten deutlich an Gewicht, da sich gerade seine beiden ersten Elemente mit diesen Abgrenzungen befassen. Klar ist, dass nur Daten und Informationen, welche sich auf eine konkrete Person beziehen, vom Schutz erfasst sein sollen. Klar ist auch, dass es sich bei Informationen und Daten nicht um dasselbe handelt, auch wenn es der Einfachheit halber gerne angenommen wird.<sup>299</sup> Es scheint zumindest auf den ersten Blick einleuchtend, dass bei Informationen nicht das gleiche Mass an Schutzbedürftigkeit bejaht werden kann wie bei manifestierten und damit unendlich vervielfältigbaren Personendaten. Der Grund dafür kann im überaus flüchtigen Charakter von Informationen gesehen werden, welcher das Verhalten der betroffenen Personen nicht im gleichen Masse zu beeinflussen vermag wie feste – und damit nicht widerlegbare – Daten.<sup>300</sup> Dennoch ist zu beachten, dass aus flüchtigen Informationen jederzeit handfeste Daten entstehen können, der «Aggregatzustand Information» somit für sich allein das Gefahrenpotential für die betroffenen Personen nicht in jedem Falle schmälert.<sup>301</sup> Es wäre unsinnig, würde die Bekanntgabe der Information «Frau Soundso befindet sich in der psychiatrischen Abteilung» unter den Schutz der informationellen Selbstbestimmung fallen, wenn die

---

<sup>298</sup> MAYER-SCHÖNBERGER, S. 59 f.

<sup>299</sup> Zur Abgrenzung Daten/Informationen siehe Kapitel IV, Ziffer 6.2 und 6.3.

<sup>300</sup> Siehe hierzu Kapitel V, Ziffer 5.2.

<sup>301</sup> Vgl. ALBERS, Informationelle Selbstbestimmung, S. 142 f.

Bekanntgabe durch ein Schreiben erfolgt (= Qualifikation als Datum), aber nicht wenn sie durch ein unaufgezeichnetes Telefonat erfolgt (= Qualifikation als Information).<sup>302</sup> Bereits das dritte Element der Persönlichkeitsnähe ist jedoch wieder zu hinterfragen. MAYER-SCHÖNBERGER macht hier das Beispiel, dass die Haarfarbe eines Menschen weniger stark seine Persönlichkeit tangiere als die Information über seinen Gesundheitszustand und so dem ersteren die Schutzwürdigkeit zu versagen wäre. Erinnern wir uns an die Bestrebungen Hitlers, die «arische Rasse» zu fördern, indem andere «Rassen» eliminiert wurden, so war das Vorhandensein einer dunklen Haarfarbe ein Indiz für dessen Nichtzugehörigkeit zu dieser erkorenen «Rasse» und die diesbezügliche Information keinesfalls harmlos.<sup>303</sup> Der Vermerk in der Krankenakte «Frau Soundso fühlt sich bei bester Gesundheit» wirft dagegen für sich allein noch kein hohes Gefährdungspotential auf. Weshalb die Marktfähigkeit ein weiteres Element bezüglich der Bejahung der Schutzwürdigkeit sein soll, ist der hier vertretenen Ansicht nach ebenfalls nicht ersichtlich, geht es doch letztlich um den Schutz der Persönlichkeit und nicht um den Schutz vermögenswerter Güter, auch wenn ein solcher evt. den Schutz der Persönlichkeit fördern könnte (siehe dazu Kapitel VI, Ziffer 5.2). Auch das fünfte von ihm genannte Element, bezogen auf die Subjekt-Objekt-Relation von juristischen Personen, vermag der hier vertretenen Auffassung nach die Schutzbedürftigkeit von Personendaten weder zu belegen noch zu verneinen. Wie BONDOLFI richtig bemerkt hat, geht es um die Bewahrung jener Informationen, «welche, falls öffentlich zugänglich, die Identität und die Selbsteinschätzung einer Person tief verletzen würden».<sup>304</sup> Da sich solche Daten und Informationen nur sehr schwer generalisierbar ausmachen lassen, muss – zumindest auf Verfassungsebene – der Schutzbedarf für alle personenbezogenen Daten und Informationen bejaht werden.<sup>305</sup>

---

<sup>302</sup> Zur Interpretation von «Bearbeiten» nach Art. 3 lit. e DSGVO siehe Kapitel VI, Ziffer 4.1.3.

<sup>303</sup> Es sei hier daran erinnert, dass gerade harmlos erscheinende Physionomiemerkmale immer wieder ein enormes Gefährdungspotential für die Betroffenen aufwiesen, so wurden im Mittelalter tausende von Frauen getötet nur weil sie das «Hexenmerkmal» rote Haare hatten (PÖTZL/HEYDENREUTER/KOHLBERGER, S. 200) und gegen Ende des vorletzten Jahrhunderts war es noch üblich Mörder an ihrer Adlernase zu erkennen (LOMBROSO, S. 230).

<sup>304</sup> BONDOLFI, S. 130.

<sup>305</sup> Vgl. SCHERTZ/HÖCH, S. 31.

## 9 Résumé und Überleitung

Die vorangehenden Überlegungen zum – wörtlich verstandenen – Schutzbedarf eines Rechts auf informationelle Selbstbestimmung haben gezeigt, dass eine solche garantierende Entscheidungsfreiheit des einzelnen in Bezug auf seine Daten und Informationen eine wesentliche Voraussetzung für die Privatheit darstellt. Diese wiederum ist eine grundlegende Bedingung für die Entwicklung und Entfaltung der Persönlichkeit des einzelnen, wozu die (Mit-)Bestimmung des Bildes, welches er nach aussen abgeben möchte, aber auch seine sozialen Rollen und Beziehungen, welche dadurch definiert und aufrecht erhalten werden, gehören. Diese freie Entfaltung der Persönlichkeit ist wiederum unabdingbar für die Ausbildung selbstbestimmter Individuen, welche, auch wenn sie manchmal nicht ganz dem Ideal entsprechen, doch die Voraussetzung menschlicher Interaktion bilden und das Fundament einer freiheitlichen Staatsordnung und einer auf Wettbewerb fundierten Wirtschaft darstellen. Damit dürften genügend Argumente für die Befürwortung der Existenzberechtigung eines Grundrechts auf informationelle Selbstbestimmung vorliegen.<sup>306</sup>

Die aufgeworfene Frage, ob jede auf eine Person bezogene Information und jedes auf eine Person bezogene Datum in den Schutzbereich fällt, muss ebenfalls bejaht werden, da das Gefährdungspotential für die Betroffenen nicht in jedem Falle mit dem «Aggregatzustand Information» ausgeschlossen werden kann. Dies bedeutet jedoch nicht, dass einem solchen Recht genereller Vorrang zu gewähren ist oder dass Geschwätz über andere Personen per se verboten wäre. Es bedeutet aber immerhin, dass insbesondere der Gesetzgeber festlegen muss, welche Art von personenbezogenen Informationen und Daten von wem wie bearbeitet werden dürfen.<sup>307</sup> Es bedeutet auch, dass wir uns aufgrund der Phänomene Datum und Information damit abfinden müssen, dass der Gesetzgeber nicht alles normieren kann (und auch nicht soll) und dass wir bis zu einem gewissen Punkt akzeptieren müssen, dass es, unabhängig von der Rechtslage, immer wieder zu einem Informationsungleichge-

---

<sup>306</sup> Vgl. EVERS, S. 39 f., diese «Kaskade» muss im Hinterkopf behalten werden, wenn im Folgenden von Gefährdung der Privatheit oder der Persönlichkeit gesprochen wird, da das eine auf dem anderen aufbaut und wiederum Grundvoraussetzung für ein selbstbestimmtes Individuum etc. ist.

<sup>307</sup> Siehe dazu Kapitel IV, Ziffer 3.

wicht kommen kann, in dem Sinne, dass andere Personen über Informationen und Daten zu einer Person «verfügen», ohne dass die betroffene Person dies möchte. Die Tatsache, dass dies passieren kann und wird, bedeutet jedoch nicht, dass die Gesellschaft als solche ein derartiges Verhalten gutheissen muss und die Rechtsordnung deshalb bestimmte Verhalten nicht unter Strafe stellen kann respektive das Recht, über die die eigene Person betreffenden Daten und Informationen zu bestimmen, nicht schützen muss. Mit den Worten ALBERS: «Dass die Informationshandlungen anderer von der betroffenen Person faktisch nicht beherrschbar sind, hindert nun keineswegs daran, in Rechtsvorschriften rechtlich begründete Einflussmöglichkeiten verankert zu sehen.»<sup>308</sup> Es scheint der Autorin nach der vorangegangenen Schutzbedarfsanalyse deshalb auch nicht mehr eine Frage zu sein, ob ein solches Recht auf informationelle Selbstbestimmung existieren *muss*, sondern vielmehr *wie* wir einem solchen Recht zum Durchbruch, zur grösserer Realitätsnähe und zur verbesserten Durchsetzbarkeit verhelfen können.

---

<sup>308</sup> ALBERS, Informationelle Selbstbestimmung, S. 132.



## **VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung**

Da die im Kapitel IV ausgewiesenen Kritikpunkte auch in Anbetracht des ausgewiesenen Schutzbedarfs ihre Berechtigung nicht einbüßen, sollen im Folgenden verschiedene Vorschläge, Ansätze und Gedanken beleuchtet werden, die dem Grundrecht auf informationelle Selbstbestimmung zu verbesserter Umsetzung und Handhabung verhelfen sollen. Dabei werden Ideen aufgezeigt, welche das Konstrukt des informationellen Selbstbestimmungsrechts entweder neu in der Rechtslandschaft einzuordnen versuchen oder aber die Schaffung von Waffengleichheit zwischen Datenbearbeiter und betroffenen Personen im Fokus haben. Die dargelegten Vorschläge, Ansätze und Gedanken stellen weder eine abschliessende Auflistung dar, noch können die einzelnen Ideen umfassend beleuchtet oder gar abschliessend beurteilt werden. Vielmehr geht es darum aufzuzeigen, dass unterschiedlichste Ansätze – alleine oder in Kombination – denkbar sind, und damit den Nachweis zu liefern, dass sich die Lehre der Probleme rund um das Recht auf informationelle Selbstbestimmung sehr wohl bewusst ist, die Wichtigkeit desselben sowie die diesbezüglich vorhandenen Gefahren anerkennt und um Lösungen bemüht ist.

### **1 Bessere Konturierung der relevanten Grundrechte**

Der Selbstbestimmung des einzelnen hinsichtlich des Umgangs mit seinen Daten ist, wie in der Schutzbedarfsanalyse<sup>309</sup> ausführlich dargelegt wurde, essentiell für die Ausbildung selbstbestimmter Individuen. Die Aufsplitterung und selbstständige Normierung verschiedener Teilgehalte der persönlichen Freiheit mit der Verfassungsrevision von 1999, kumuliert in der unglücklichen Implementierung und Formulierung eines Grundrechts auf informationelle Selbstbestimmung, haben jedoch zu einer Schmälerung des notwendigen Schutzes des einzelnen in Bezug auf den Umgang mit seinen Daten geführt, da erhebliche *Rechtsunsicherheit* darüber besteht, welcher

---

<sup>309</sup> Kapitel V.

Anspruch unter welchen Artikel subsumiert werden kann und ob ein solcher Anspruch überhaupt geschützt ist.<sup>310</sup> Es scheint deshalb für eine bessere Handhabung und eine bessere Durchsetzung des Rechts auf informationellen Selbstbestimmung unumgänglich, die Art. 10 und 13 BV mindestens für diesen Bereich genau voneinander abzugrenzen und in Bezug auf die Gewährleistung des aufgezeigten Schutzbedarfs deutlicher zu konturieren.

### **1.1 Privatsphäre oder persönliche Freiheit?**

Der Schutz der Privatsphäre nach Art. 13 Abs. 1 BV gewährleistet einen Raum für die private Lebensgestaltung, der vom Staat geachtet und vor unerwünschten Eingriffen wirksam geschützt wird und in dem grundsätzlich jeder Mensch selber entscheiden kann, ob und wem er *persönliche Lebenssachverhalte* preisgibt.<sup>311</sup> Nach dem Ansatz von MÜLLER/SCHEFER ist der Anspruch auf Schutz der Privatsphäre als Recht «allein gelassen zu werden» zu verstehen,<sup>312</sup> wobei der Staat nicht nur selbst den diesbezüglichen Entscheid des einzelnen zu achten hat, sondern ebenfalls dafür besorgt sein muss, dass auch private Akteure dies tun.<sup>313</sup> Schwierigkeiten bereiten in diesem Kontext vor allem die Beantwortung der Fragen, wie sich diese private Sphäre von der Öffentlichkeit abgrenzen lässt, wann der einzelne solche privaten Sphären beanspruchen kann und welches die Lebensbereiche sind, die für die freie Entfaltung des Individuums so zentral sind.<sup>314</sup>

#### **1.1.1 Das Zwiebelmodell**

Bei der Abgrenzung des Privaten vom Öffentlichen wird vor allem das Schalen- oder Zwiebelmodell angewendet. Nach RÖSSLER wäre demzufolge in einen Bereich der persönlichen Intimität und Privatheit zu unterscheiden, demgegenüber alles andere als öffentlich gilt, und dem eine zweite Schicht, diejenige des klassischen Privatbe-

---

<sup>310</sup> Vgl. GÄCHTER/EGLI, RZ 61.

<sup>311</sup> In Anbetracht der heutigen Kommunikationswege und -netze müssen darunter wohl ebenfalls virtuelle Räume sowie der E-Mail- oder sonstige digitale Fernmeldeverkehr zu subsumiert werden.

<sup>312</sup> MÜLLER/SCHEFER, S. 140.

<sup>313</sup> BELSER, Instrumente, S. 31 f.

<sup>314</sup> Vgl. GÄCHTER/EGLI, RZ 67.

reichs, nämlich der Familie, folgt.<sup>315</sup> In ähnlicher Weise geht das Bundesgericht davon aus, dass sich das Leben eines jeden Menschen in drei Lebenskreisen (= Sphären) unterteilen lässt: Die *Intimsphäre* als innerster Kern, die *Privatsphäre* als mittlerer Kreis und die *Gemeinsphäre* als äusserster Kreis.<sup>316</sup> Die Intimsphäre umfasst dabei jene persönlichen Angelegenheiten, welche Dritten verwehrt werden sollen. Dabei sind vom Ausschluss der Kenntnis alle Personen betroffen, welchen der einzelne die jeweilige Tatsache nicht selbst anvertraut hat. Während sodann zur Privatsphäre jene Lebensvorgänge gehören, «die man typischerweise nur einem kleinen, begrenzten Kreis von Personen (z.B. Verwandten und Freunden) offenlegt,»<sup>317</sup> umfasst die Öffentlichkeitssphäre jene Informationen, die allen Personen bekannt sind oder bekannt gemacht werden können.<sup>318</sup>

Die Gewährleistung solcher privater Sphären ist, wie bei der Schutzbedarfsanalyse aufgezeigt wurde, eine elementare Voraussetzung dafür, dass sich der einzelne frei entfalten und dadurch seine tragende Rolle als selbstbestimmtes Individuum in der Gesellschaft wahrnehmen kann.<sup>319</sup> Daten und Informationen aus diesen abstrakt definierten Sphären sind jedoch per se nicht von Art. 13 Abs. 1 BV geschützt, da jede Person die Entscheidung, welches Datum welcher Sphäre zugehören soll, individuell und nach subjektiven Kriterien trifft und keine abstrakte Zuordnung bestimmter Daten und Informationen zu einer bestimmten Sphäre erfolgen kann. Nach GÄCHTER/EGLI würde mit der Ansicht, dass mit der Gleichstellung von Privatsphäre und der aus ihr stammenden Daten und Informationen gar ein «Kategorienfehler» begangen, da es sich nicht um das gleiche Schutzgut handle. Demnach können Daten und Informationen aus der Privatsphäre diese ebenso wenig verletzen wie Daten und Informationen über den Körper die physische Integrität verletzen können.<sup>320</sup> Dieser Ansicht ist jedoch nur bedingt zu folgen. Richtig ist, dass Daten und Informationen aus der Privatsphäre nicht das *Schutzgut* des Rechts auf Privatsphäre darstellen. Die geschützten privaten Bereiche können aber sehr wohl durch Daten und Informationen aus

---

<sup>315</sup> RÖSSLER, S. 18.

<sup>316</sup> Statt vieler: BGE 97 II 97 ff. (100 f.), E. 3; BGE 118 IV 41 ff. (45), E. 4.

<sup>317</sup> BRÜCKNER, RZ 484.

<sup>318</sup> BRÜCKNER, RZ 484 f.

<sup>319</sup> Siehe GÄCHTER/EGLI, RZ 69.

<sup>320</sup> GÄCHTER/EGLI, RZ 70.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

diesen Bereichen resp. durch den Umgang mit solchen tangiert werden.<sup>321</sup> Beispielsweise sind Aufzeichnungen aus den privaten Räumen, seien es Fotos oder Filmchen, die eine Person bei intimen Angelegenheiten wiedergeben und zu deren Herstellung und Weiterverwendung sie keine Einwilligung gegeben hat, sehr wohl geeignet, die Privatsphäre, als einen dem Individuum zustehenden Raum, in dem nur die von ihm ermächtigten «Zutritt» haben, zu verletzen. Als Beispiel sei hier an die Stalkerin zu denken, die den Mann ihrer Träume durchs Fenster hindurch filmt, wie er aus der Dusche steigt. Das Filmchen gibt eine Handlung in einem geschützten privaten Raum wieder, das Recht in Ruhe gelassen zu werden ist dadurch verletzt. Oder um das Beispiel der psychischen Integrität aufzunehmen: Daten und Informationen betreffend den Körper vermögen zwar nicht die physische Integrität zu verletzen, aber sehr wohl die psychische. Nehmen wir an, einer Frau mit Kinderwunsch wird mitgeteilt, dass sie keine Kinder bekommen kann, da sie an einer schweren Erkrankung ihrer Eierstöcke leidet und diese unmittelbar entfernt werden müssen. Diese Information kann ihr psychisches Wohlbefinden erheblich beeinträchtigen, was letztlich ja gerade die Rechtfertigung für das mittlerweile umstrittene, aber immer noch beliebte therapeutische Privileg<sup>322</sup> darstellt.<sup>323</sup> Daten und Informationen sind auch nicht Schutzobjekt der Religionsfreiheit und doch kann die Religionsfreiheit tangiert sein, wenn Daten, welche Personen bei religiösen Riten wiedergeben, an ein «falsches» Publikum geraten und die Betroffenen die ihnen zustehende Freiheit, ihre Religion auszuleben, nicht mehr wahrnehmen. Diese Beispiele zeigen, dass Daten und Informationen nicht Schutzobjekt einer verfassungsrechtlichen Garantie sein müssen, damit durch den Umgang mit ihnen gleichwohl der jeweilige Schutzbereich tangiert wird. Ihre jeweilige Charakteristik und die Möglichkeiten, mit ihnen umzugehen, sind viel zu komplex, um ihren Wirkungskreis auf einzelne Grundrechte fixieren zu können.

---

<sup>321</sup> Nach ALBERS schliesst das inhaltliche Konzept einer privaten Sphäre den Schutz in Bezug auf die Gesprächsinhalte oder Daten ein, die in dieser Sphäre entstehen. (ALBERS, Informationelle Selbstbestimmung, S. 610).

<sup>322</sup> Der Arzt geht dabei davon aus, dass der Patient mit allen Informationen bezüglich seiner Physis auf der psychischen Ebene nicht fertig wird und die vollständige Aufklärung über alle Informationen den Behandlungsverlauf negativ beeinträchtigen würde, weshalb er ihm – quasi zu seinem eigenen Besten - nur einen Teil der Information bekannt gibt.

<sup>323</sup> Vgl. WARREN/BRANDEIS, S. 193 ff., wonach das Eindringen in den privaten Bereich dem Betroffenen mehr Schmerzen und Sorgen bereite, als es durch eine körperliche Verletzung möglich sei.

Um wieder beim Schutz der Privatsphäre anzuknüpfen: Die Definition einer oder mehrere solchen privaten Sphären bleibt schwierig, denn sie ist/sind «kein(e) Wesen, welche(n) ein Eigenwert an sich zukäme»<sup>324</sup> und es liegt auf der Hand, dass diese abstrakt definierten Bereiche nicht zwingend mit den individuell als schützenswert empfundenen übereinstimmen müssen.<sup>325</sup>

### 1.1.2 Privatheit – Privacy

Diesen Schwierigkeiten versuchen verschiedene Autoren zu begegnen, indem sie nicht den Schutz einer privaten Sphäre in den Vordergrund stellen, sondern den Schutz der Privatheit im Sinne von *Vertraulichkeit*. Diese Idee schliesst nicht an die der Privatsphäre zugrunde liegende Ja/Nein-Konzeption an, sondern anerkennt, dass das Individuum in gesellschaftlichen Rollen und Beziehungen lebt und je nachdem Daten und Informationen bekannt gibt oder nicht. Denn wie es DRUEY formuliert hat, ist nach dieser Theorie nicht die Geheimheit von Informationen und Daten zu schützen, sondern der Umstand, «dass jede Äusserung ihre implizite Reichweite hat.»<sup>326</sup> Auch die im common law traditionsreich geschützte Privacy ist heute nicht mehr nur als Schutz einer Sphäre zu verstehen, die dem staatlichen Zugriff entzogen ist.<sup>327</sup> WESTIN definiert den Begriff der Privacy etwa als «the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.»<sup>328</sup> Eine ähnliche Definition kommt von FRIED: «Privacy is (...) the control we have over information about ourselves.»<sup>329</sup> Nach RÖSSLER bedeutet Schutz von Privatheit Schutz vor unerwünschtem Zutritt anderer, wobei Zutritt sowohl konkret im Sinne von Zugang zu einem Raum bedeuten kann als auch metaphorisch, in dem Sinn, dass jemand die *Kontrolle* darüber hat, wer welchen Wissenszugang zu ihm hat.<sup>330</sup> Es gilt etwas dann als privat, wenn man selbst den Zugang zu diesem «etwas» kontrollieren kann. Das «kann» ist zu verste-

---

<sup>324</sup> BONDOLFI, S. 131.

<sup>325</sup> So auch BONDOLFI, S. 131.

<sup>326</sup> DRUEY, Strukturelle Schwäche, S. 149.

<sup>327</sup> Siehe BONDOLFI, S. 128 ff.

<sup>328</sup> WESTIN, S. 7.

<sup>329</sup> FRIED, S. 482.

<sup>330</sup> RÖSSLER, S. 23 f.

hen im Sinne von «kann und/oder sollte und/oder darf», denn nicht immer, wenn jemand faktisch den Zugang zu etwas kontrollieren kann, ist dieses Etwas auch privat. Der Schwerpunkt all dieser Definitionen liegt auf der Kontrolle, auf der Idee des unerwünschten «Zutritts» anderer zu einem für sich als privat definierten Etwas und damit nicht wie bei der Idee einer Privatsphäre in der Trennung zwischen einem einzelnen Individuum auf der einen und einer Öffentlichkeit auf der anderen Seite.<sup>331</sup> Demnach sind Daten/Information einer Person als privat anzusehen, wenn diese den Zugang dazu kontrollieren kann und/oder können sollte. Das und/oder ist hier besonders relevant, da die Person faktisch den Zugang nicht immer kontrollieren kann, das Element «sollte» aber dafür Sorge trägt, dass klar ist, dass eigentlich für die legitime Verbreitung dieser Informationen die Zustimmung der betroffenen Person erforderlich wäre.<sup>332</sup> In diesem Sinne hat sich auch der Begriff der «informationellen Privatheit» bei diversen Autoren etabliert.<sup>333</sup>

Diese Privatheit im Sinne der Vertraulichkeit von personenbezogenen Daten und Informationen wird nach GÄCHTER/EGLI von der persönlichen Freiheit nach *Art. 10 Abs. 2 BV* geschützt.<sup>334</sup> Der hier vertretenen Meinung nach stellt die Vertraulichkeit einer Information oder eines Datums jedoch keine elementare Erscheinungsform der Persönlichkeitsentfaltung und damit kein Schutzobjekt der persönlichen Freiheit dar. Nach VAN SPYK lassen sich die Persönlichkeitsrechte, welche durch die persönliche Freiheit geschützt werden, in zwei *Kategorien* unterteilen: Während die erste Kategorie die persönliche Integrität als solche vor äusseren Beeinträchtigungen schützt (insbesondere Integritätsschutz, Zustand, Sein, Freiheit von), schützt die zweite Kategorie die Selbstbestimmung eines Individuums über ihre Lebensgestaltung und damit auch «die Verfügungsfreiheit des einzelnen über die Gehalte der persönlichen Integrität (Aktivitätsschutz, Handlung, Tun, Unterlassen, Freiheit zu)».<sup>335</sup> Dabei gewährleistet die persönliche Freiheit in ihrer aktiven Ausprägung sowohl den Schutz der Willensbildung (Entscheidungsfreiheit) als auch der freien Willensbetätigung

---

<sup>331</sup> RÖSSLER, S. 24.

<sup>332</sup> RÖSSLER, S. 24.

<sup>333</sup> RÖSSLER, S. 25, AEBI-MÜLLER, RZ 496 f.; siehe auch RUDIN, Erosion, S. 415 ff.

<sup>334</sup> GÄCHTER/EGLI, RZ 71.

<sup>335</sup> VAN SPYK, S. 30 f.

(Handlungsfreiheit).<sup>336</sup> Die Privatheit im Sinne der Vertraulichkeit kann nicht unter die hier beschriebenen Schutzgüter subsumiert werden, sie stellt eine gänzlich andere Art Schutzgut dar. Das Recht auf Privatheit schützt eine Handlung/ein Datum aufgrund dessen, dass sie/es eine Person als privat definiert hat. Damit eine Person einem Datum o.ä. diesen «Status» privat jedoch überhaupt verleihen kann, muss ihm die Rechtsordnung zugestehen, frei zu entscheiden, ob ein solches Etwas privat oder öffentlich sein soll. Das Selbstbestimmungsrecht nach Art. 10 Abs. 2 BV verleiht dem einzelnen das Recht, seinen Lebenswandel nach den eigenen Vorstellungen zu gestalten, wozu auch die Freiheit, über grundrechtlich gewährleistete Schutzbereiche zu «verfügen» und so beispielsweise auch in ihre Beeinträchtigung einzuwilligen oder auf ihre Ausübung zu verzichten, gehört.<sup>337</sup> Eine allgemeine Handlungsfreiheit begründet die Bestimmung zwar nicht, aber zumindest die elementaren Erscheinungsformen der Persönlichkeitsentfaltung werden geschützt. Als solche gliedert sich der Anspruch auf Selbstbestimmung über den Umgang mit den eigenen Daten und Informationen – gleich wie die Freiheit, über Eingriffe in die körperliche oder geistige Unversehrtheit selber zu bestimmen – mühelos in die bereits anerkannten Ansprüche des Rechts auf persönliche Freiheit ein.<sup>338</sup> Es ist also nicht die Vertraulichkeit eines bestimmten Datums, welche von Art. 10 Abs. 2 BV geschützt wird, sondern die (Selbst-)Bestimmung darüber, ob ein die eigene Person betreffendes Datum oder Information einer bestimmten Person gegenüber vertraulich sein soll oder nicht.

Es ist hier allerdings zu konstatieren, dass auch die Auslegung, dass es sich bei der informationellen Selbstbestimmung um eine von Art. 10 Abs. 2 BV geschützte elementare Voraussetzung der Persönlichkeitsentfaltung handelt, ihre *Tücken* aufweist.

---

<sup>336</sup> VAN SPYK, S. 34.

<sup>337</sup> VAN SPYK, S. 34 f.

<sup>338</sup> Vgl. BELSER, Instrumente, S. 30; auch STEINMÜLLER ET AL. haben in ihrem Gutachten die informationelle Selbstbestimmung im Grundrecht auf freie Entfaltung der Persönlichkeit verortet. (STEINMÜLLER ET AL., S. 85); a.M. DRUEY, demgemäss sich der traditionelle Kern des subjektiven Rechts gegen Information - das Persönlichkeitsrecht - als nicht richtigen Platz erweist, da jedes Recht Informationen zurückzuhalten sich auf eine soziale Wertung stützen muss, wonach das Zurückhalten der Verbreitung vorzuziehen ist. Dies sei aber die Problemstellung bei der Güterverteilung, womit die Analogie zum Sachenrecht und nicht zum Persönlichkeitsrecht bestehe (DRUEY, Information, S. 361 ff).

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

So dienen beispielsweise die typischen Schutzgüter von Art. 10 Abs. 2 BV – die körperliche und geistige Unversehrtheit – unmittelbar der persönlichen Freiheit, wohingegen die informationelle Selbstbestimmung durch ihr Schutzgut der Entscheidungsfreiheit über die eigenen Daten und Informationen dem Schutz des Privaten dient, und erst dieses Schutzgut befindet sich genau betrachtet auf der gleichen Flughöhe wie die physische und psychische Integrität. Gleichwohl scheint es der Autorin aufgrund der dargelegten Überlegungen am sachdienlichsten, die informationelle Selbstbestimmung im oben dargestellten Sinne als Teil der persönlichen Freiheit zu betrachten.<sup>339</sup> In diesem Sinne auch das Zitat von WARREN/BRANDEIS: «The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.»<sup>340</sup>

### **1.2 Art. 13 Abs. 2 BV - Schutz vor Missbrauch persönlicher Daten**

Vor dem Hintergrund der mit dem herrschenden Verständnis auf informationelle Selbstbestimmung verbundenen Schwierigkeiten legen GÄCHTER/EGLI Art. 13 Abs. 2 BV nicht im Sinne einer dem Individuum zustehenden Dispositions- oder Entscheidungsfreiheit aus. Art. 13 Abs. 2 BV gewähre vielmehr – eng am Wortlaut angelehnt – einen Anspruch auf Schutz vor Missbrauch der die eigene Person betreffenden Daten.<sup>341</sup> Die Vertreter dieser Meinung anerkennen ebenso wie die Vertreter eines informationellen Selbstbestimmungsrechts, dass der einzelne in seiner freien Persönlichkeitsentfaltung bedroht ist, wenn er nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiss.<sup>342</sup> Dieser Gefahr sei aber nicht durch eine dem Individuum selbst zustehende Entscheidungsfreiheit zu begegnen – worin GÄCHTER/EGLI ein quasi Informationsverbot sehen –, sondern durch *Begrenzung* der Daten- und Informationsflüsse mittels vom Gesetzgeber definierter Re-

---

<sup>339</sup> Ähnlich auch BELSER, dergemäss einschneidende Formen der Datenbearbeitung den Kerngehalt der persönlichen Freiheit betreffen können, da schwere Beeinträchtigungen der Urteils- und Entscheidungsfähigkeit die Autonomie des Menschen und seine Würde gefährden (BELSER, Instrumente, S. 30); vgl. WOLLENTEIT, S. 248 oder SAINT-MONT, S. 96.

<sup>340</sup> WARREN/BRANDEIS, S. 205.

<sup>341</sup> GÄCHTER/EGLI, RZ 13.

<sup>342</sup> GÄCHTER/EGLI, RZ 14.



## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

geln.<sup>343</sup> Ziel von Art. 13 Abs. 2 BV sei der Schutz vor staatlichem Umgang mit Personendaten als solchem und eben nicht der Schutz inhaltlich bestimmter Personendaten.<sup>344</sup> Damit schütze Art. 13 Abs. 2 BV eine *strukturelle oder institutionelle Dimension* des verfassungsrechtlichen Persönlichkeitsschutzes. Es verhalte sich ähnlich wie mit den allgemeinen Verfahrensgarantien nach Art. 29 BV: Die Ansprüche der Betroffenen ergeben sich grundsätzlich aus dem einfachen Gesetzesrecht (eidgenössisches und kantonale Datenschutzgesetze). Um eine missbräuchliche Datenbearbeitung handle es sich dementsprechend nach der Meinung von Altbundesrat Koller, sobald die Angaben des Datenschutzgesetzes nicht eingehalten werden.<sup>345</sup> Eine unmittelbare Berufung auf Art. 13 Abs. 2 BV sei erst möglich, wenn das einfache Gesetzesrecht den grundlegenden Anforderungen des verfassungsrechtlichen Schutzes (den Minimalstandards) nicht entspricht.<sup>346</sup> Die Zulässigkeit staatlicher Datenbearbeitungen richte sich somit nicht nach dem Willen des Betroffenen, massgeblich sei nur, ob der staatliche Umgang mit Personendaten den Minimalstandards entspricht<sup>347</sup> und somit als nicht missbräuchlich zu werten ist. Nach diesem Verständnis hat also der *Gesetzgeber* in erster Linie dafür Sorge zu tragen, dass der Umgang mit Personendaten nicht «weitgehend ungebunden, unbegrenzt, undurchschaubar und an den Betroffenen vorbei verläuft.»<sup>348</sup> Dafür muss er sich an gewisse Vorgaben halten. Genannt werden etwa sachgerechter und transparenter Umgang mit Personendaten, Gewährleistung individueller Kenntnismöglichkeit und Einflusschancen sowie die Institutionalisierung adäquater Kontrollen.<sup>349</sup>

---

<sup>343</sup> GÄCHTER/EGLI, RZ 15.

<sup>344</sup> GÄCHTER/EGLI, RZ 26.

<sup>345</sup> Votum BR Koller Arnold, AmtlBull NR 1998, S. 694.

<sup>346</sup> GÄCHTER/EGLI RZ 48.

<sup>347</sup> GÄCHTER/EGLI, RZ 55.

<sup>348</sup> GÄCHTER/EGLI, RZ 38 f.

<sup>349</sup> ALBERS, Umgang, RZ 75 ff.

### **1.3 Zusammenführung und Würdigung**

#### **1.3.1 Wenige Überlappungen – kohärenterer Grundrechtsschutz**

Nach BELSER würde eine derartige Interpretation des Art. 13 Abs. 2 BV zu weniger Überlappungen und zu einem kohärenteren Grundrechtsschutz führen. Art. 13 Abs. 1 BV würde dann den Datenschutz ergänzen, wenn es um besonders empfindliche Bereiche gehe, wie Wohnräume oder die Kommunikation. Art. 10 Abs. 2 BV käme zusätzlich zum Zuge, wenn die psychische Integrität von Menschen oder ihre Entscheidungsfähigkeit in Frage stehe.<sup>350</sup> BELSER ist insoweit zuzustimmen, als dass durch die Konkretisierung und Zuweisung der einzelnen Schutzpositionen hinsichtlich des Umgangs mit Personendaten und -informationen zu den jeweiligen Grundrechtsgarantien von Art. 10 Abs. 2, Art. 13 Abs. 1 und Abs. 2 BV ein breitgefächelter und somit gut fundierter Schutz des einzelnen gewährleistet werden kann. Während Art. 10 Abs. 2 und Art. 13 Abs. 1 BV dem einzelnen unmittelbare Rechte zugestehen, richtet sich Art. 13 Abs. 2 BV in erster Linie an den Gesetzgeber und verlangt von ihm das Nötige, um den Schutz zu gewährleisten. So kommt jedem der drei Grundrechte sein eigener Schutzgehalt zu, welcher sich einigermaßen klar von den anderen Schutzpositionen unterscheiden lässt und so im entsprechenden Falle selbständig angerufen werden kann.

Diese Auslegung hätte für sich, dass sie einerseits das Recht des einzelnen achtet, mit Informationen und Daten, welche sein persönliches Leben betreffen, so umzugehen, wie es ihm beliebt und ihm damit eine wesentliche Voraussetzung für die freie Entfaltung seiner Persönlichkeit schafft. Andererseits berücksichtigt sie, dass es vom Staat festgelegte Grenzen gibt, in denen die Selbstbestimmung ausgelebt werden kann und die allgemein gültige Vorgaben bezüglich grundrechtskonformer Daten- und Informationsbearbeitung machen.<sup>351</sup> Diese staatlich gesetzten Grenzen – oder besser Rahmenbedingungen – sind essentiell, denn sie sorgen u.a. dafür, dass der einzelne sein Recht auf informationelle Selbstbestimmung nicht allzu schnell in die Waagschale wirft, weil er deren Wert als Grundvoraussetzung für seine Autonomie

---

<sup>350</sup> BELSER, Instrumente, S. 37.

<sup>351</sup> Vgl. BONDOLFI, S. 131, vgl. auch GARSTKA, S. 159.

nicht erkennt.<sup>352</sup> Denn wie vorne ausgeführt, handelt es sich beim Grundrecht auf informationelle Selbstbestimmung nicht nur um ein individuelles Recht, sondern auch um eine Grundvoraussetzung für eine funktionierende Gesellschaft, Demokratie und Wirtschaft.<sup>353</sup> Somit ist klar, dass die Verantwortung für das Interesse an der Gewährleistung der informationellen Selbstbestimmung nicht nur beim Individuum liegen kann und darf, sondern dass der Staat im öffentlichen Interesse gewisse Vorgaben für den Umgang mit Personendaten machen muss.

Damit wäre auch das wenig diskutierte Verhältnis zwischen Datenschutzgesetzen, welche sich nach GARSTKA in der Regel als Erlaubnismechanismen für die Verarbeitung personenbezogener Daten entpuppten,<sup>354</sup> und dem Recht auf informationelle Selbstbestimmung geklärt: Es besteht ein Grundrecht auf Entscheidungsfreiheit bezüglich des Umgangs mit den die eigene Person betreffenden Daten. Die vom Staat vorgegebenen Rahmenbedingungen zur Ausübung des Grundrechts dienen einerseits der verfassungskonformen Erfüllung staatlicher Aufgaben, andererseits dienen sie im Hinblick auf eine an selbstbestimmten Individuen orientierten Gesellschaft aber auch dazu, dass der einzelne sein Persönlichkeitsrecht nicht zu billig verkauft.<sup>355</sup>

### 1.3.2 Missbrauchsschutz reicht nicht

Die komplette Negierung eines Grundrechts auf Selbstbestimmung bezüglich des Umgangs mit den eigenen Personendaten und die Idee, den diesbezüglichen Schutz alleine über das Missbrauchsverbot nach Art. 13 Abs. 2 BV abzuwickeln, ist der hier vertretenen Meinung nach abzulehnen. Nebst der Überzeugung, dass dem aufgezeigten *Schutzbedarf* mit einem reinen Missbrauchsverbot nicht adäquat beizukommen ist, sind folgende Bedenken gegen die alleinige Existenz eines Missbrauchsverbotes anzuführen:

---

<sup>352</sup> Zum Wert des Datenschutzes siehe Kapitel V, Ziffer 6.

<sup>353</sup> RUDIN, Datenschutzaufsicht, S. 410.

<sup>354</sup> GARSTKA, S. 160.

<sup>355</sup> Vgl. ALBERS, welche die Frage aufwirft, ob es ggf. angemessener sei, die informationelle Selbstbestimmung als Komplex von Rechten aufzufassen, dessen Inhalt und Struktur noch zu verfeinern sind (ALBERS, Informationelle Selbstbestimmung, S. 163).

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

Die Aufgabe, die *Minimalstandards* näher zu umschreiben und damit Kriterien zulässiger Datenbearbeitung zu entwickeln, haben Lehre und Praxis bis heute noch nicht befriedigend gelöst,<sup>356</sup> auch wenn sich nach GÄCHTER/EGLI wichtige Anhaltspunkte für die Konkretisierung dieser Minimalanforderungen in den Datenschutzgesetzen von Bund und Kantonen sowie Lehre und Praxis hierzu finden lassen.<sup>357</sup> Bezüglich dieser Anhaltspunkte sei jedoch angemerkt, dass kaum Vergleichsmöglichkeiten vorhanden sind. Es stellt sich also die Frage, woran gemessen werden soll, ob es sich um einen sachgerechten, transparenten Umgang handelt, ob die individuelle Kenntnismöglichkeit genügend gewährleistet ist und ob die institutionalisierten Kontrollen adäquat genug sind. Und selbst wenn diese Minimalstandards besser umschrieben werden sollten, ist darauf hinzuweisen, dass die bis anhin angenommenen *Regelungsparadigmata* (eindeutige Zuordnung der Verantwortung für Abläufe am Rechner, vollständige Transparenz der Verfahren, Regelbarkeit der Abläufe unter Verwendung von Kriterien wie Erforderlichkeit, Zweckbindung etc.), welche eine relativ eindeutige Zuordnung zwischen Regelungsgegenstand, Regelungsziel und Normadressaten ermöglichten, in Anbetracht der heutigen und noch kommenden technologischen Möglichkeiten, keine Gültigkeit mehr beanspruchen können.<sup>358</sup>

Überdies muss beachtet werden, dass der Missbrauchsschutz von Art. 13 Abs. 2 BV erst in jenem *Zeitpunkt* beginnt, in dem der einzelne einen Missbrauch bezüglich der Bearbeitung seiner Daten geltend machen kann. Dies hat für den Betroffenen gleich mehrere unangenehme Folgen: Zum einen muss zuerst ein Missbrauch *eingetreten* sein, was in Anbetracht der damit einhergehenden Persönlichkeitsverletzung mehr als unbillig erscheint. Als nächstes muss der einzelne den Missbrauch *feststellen*. Dies scheint trivial, doch wer von einem Missbrauch erfahren möchte, muss zuerst einmal in Kenntnis der Datenbearbeitung als solche sein. Dies stellt weder bei Datenbearbeitungen durch öffentliche Organe, noch bei Datenbearbeitungen durch Private eine realistische Anforderung dar, da die Informationspflicht, wie gezeigt,<sup>359</sup> nur sehr eingeschränkt gilt und es dem einzelnen deshalb unmöglich ist, alle Bearbeitun-

---

<sup>356</sup> GÄCHTER/EGLI, RZ 50.

<sup>357</sup> GÄCHTER/EGLI, RZ 51.

<sup>358</sup> M.w.H GARSTKA, S. 167.

<sup>359</sup> Zur Informationspflicht siehe Kapitel III, Ziffer 2.1.

gen seiner Personendaten zu kennen. Zum anderen muss er diesen Missbrauch dann auch noch *belegen*, was eine zusätzliche Hürde darstellt. All diese Bedingungen führen dazu, dass sich der einzelne nur in Ausnahmefällen gegen staatliche und private Informationstätigkeiten wehren kann.<sup>360</sup> Diese Ausführungen verweisen alsdann zur Kritik von RUDIN, wonach ein blosses Missbrauchsverbot weniger weit geht, als die Schweiz sich völkerrechtlich durch die Ratifikation der Europaratskonvention und andere verpflichtet hat, es sei denn, Missbrauch bedeute auch ein Abweichen von den Konventionen.<sup>361</sup>

Als letzter Hinweis sei noch angebracht, dass die reine *Wortlautinterpretation* des Art. 13 Abs. 2 BV auch auslegungstechnisch zu kurz greift. Der Wortlaut stellt wohl das erste, aber dennoch nur ein Auslegungselement dar, dem nach der Rechtsprechung des Bundesgerichts keine vorrangige Bedeutung gegenüber den anderen Auslegungselementen zukommt.<sup>362</sup> Den Materialien zu Art. 13 Abs. 2 BV sind keinerlei Hinweise auf eine Einschränkung des historisch gewachsenen und unter der alten Verfassung als ungeschriebenes Grundrecht anerkannten Recht auf informationelle Selbstbestimmung zu entnehmen. Auch die Rechtsprechung ist in keiner Weise von ihrer ursprünglichen, wenn auch sehr vagen, Doktrin abgewichen. Darüber hinaus sprechen sowohl die Systematik als auch der ebenfalls von dieser Meinung anerkannte Zweck – Sicherung der freien Entfaltung der Persönlichkeit – gegen eine derart enge Auslegung von Art. 13 Abs. 2 BV. Der von den Verfechtern einer reinen Wortlautinterpretation gegen ein informationelles Selbstbestimmungsrecht vorgebrachte Vorwurf der Konturlosigkeit<sup>363</sup> greift darüber hinaus auch hier. Die Bestimmung beschreibt weder das Schutzobjekt noch den Schutzzweck eines blossen Missbrauchsschutzes überzeugend. Dies liegt wiederum an der schlicht zu kurz gehaltenen Norm, die darüber hinaus vom Wortlaut her nicht einmal die bis zu ihrer Einführung vertretene Rechtsauffassung wiedergibt.

---

<sup>360</sup> Vgl. SCHWEIZER, SG-Komm BV, N 72 zu Art. 13 BV.

<sup>361</sup> RUDIN, Risiko und Recht, S. 320

<sup>362</sup> BGE 136 V 195 ff. (203), E. 7.1.

<sup>363</sup> GÄCHTER/EGLI, RZ 36; BELSER, Datenschutzrecht, § 6 N 118.

### 1.3.3 Fazit

Eine bessere Konturierung der Teilgehalte von Art. 10 Abs. 2 und Art. 13 BV führen zu weniger Überlappungen und damit zu einem kohärenteren Grundrechtsschutz, wohingegen die komplette Negierung einer informationellen Selbstbestimmung und ein reines Abstellen auf das Missbrauchsverbot nach Art. 13 Abs. 2 BV in Anbetracht des ausgewiesenen Schutzbedarfs abgelehnt werden muss.

## 2 Unmittelbare Wirkung zwischen Privatpersonen

Aufgrund der den Grundrechten ursprünglich zugewiesenen Funktion als freiheitsrechtliche Beschränkung staatlicher Wirksamkeit<sup>364</sup> entfaltet die informationelle Selbstbestimmung ihre Wirkung primär in der Beziehung zwischen Staat und Bürger.<sup>365</sup> Das bereits erläuterte Phänomen «big data» zeigt jedoch, dass grosse globale Privatunternehmen, wie Google, Microsoft, Facebook wahrscheinlich schon lange über weit mehr Daten verfügen als dies beispielsweise klassisch genannte Überwachungsstaaten wie die DDR oder Hitler-Deutschland je getan haben.<sup>366</sup> Hierdurch verschiebt sich jedoch das gefürchtete *Machtmonopol* und damit einhergehend das Risiko einer Grundrechtsverletzung teilweise weg vom Staat und hin zu privaten Grossunternehmen. Im Hinblick auf die Risiken, welche mit den modernen Datenverarbeitungen auch und gerade durch Privatpersonen geschaffen werden (siehe dazu Kapitel V, Ziffer 5), stellt sich die Frage, ob die informationelle Selbstbestimmung nicht zumindest in einem gewissen Umfang ebenfalls zwischen Privaten unmittelbare Wirkung entfalten müsste. Dadurch könnte sie ihrer Funktion als freiheitsbewahrendes Grundrecht und ihrer Bedeutung als eine der Grundvoraussetzungen für die Entwicklung selbstbestimmter Individuen und eines auf Autonomie beruhenden Gemeinwesens gerecht werden. In diesem Sinne weist etwa auch SCHWEIZER darauf hin, dass «dort, wo unter Privaten ein erhebliches Machtgefälle besteht, das die Gewährleistung von menschlicher Würde, Freiheit und Gleichheit durch die Grundrechte

---

<sup>364</sup> GIACOMETTI, S. 243 f.

<sup>365</sup> Zur Horizontalwirkung von Grundrechten siehe Kapitel VI, Ziffer 2.

<sup>366</sup> Vgl. zur Menge der durch «big data»-Technologien anfallenden Daten MAYER-SCHÖNBERGER/CUKIER, S. 15 ff.

beeinträchtigt, oder wo von Privaten besondere Gefährdungen ausgehen», dem Staat aus den Grundrechten besondere Pflichten erwachsen.<sup>367</sup>

Die Frage, ob private Personen in ihrem privatautonomen Tätigwerden an die Grundrechte gebunden sind, wird in der Rechtsprechung und Lehre unter den Stichworten «Drittwirkung» oder «Horizontalwirkung» von Grundrechten diskutiert.<sup>368</sup> Während die *indirekte* Horizontalwirkung die Auswirkungen der Grundrechte in der Ausgestaltung des Privat- und Strafrechts sowie in der grundrechtskonformen Interpretation der genannten Rechtsgebiete, aber auch des unter Privaten wirkenden Verwaltungsrechts meint, sind mit der *direkten* Horizontalwirkung unmittelbare verfassungsmässige Rechte und Pflichten zwischen Privatpersonen gemeint.<sup>369</sup>

## 2.1 Direkte Horizontalwirkung

Die herrschende Schweizer Lehre lehnt eine direkte Horizontalwirkung der Grundrechte ab und verneint damit die Frage, ob die Grundrechte direkt eine richterliche Beurteilung der Verhältnisse unter Privaten zulassen.<sup>370</sup> Auch das Bundesgericht folgt mehrheitlich dieser *ablehnenden Haltung*.<sup>371</sup> Allerdings hat es in BGE 120 V 312 ff. anerkannt, dass eine direkte Horizontalwirkung gegeben sein kann, «wenn das Privatrecht einen grundrechtsrelevanten Bereich nicht regelt oder (echte und unechte) Lücken aufweist». <sup>372</sup> So bejaht es beispielsweise eine direkte Horizontalwirkung von Art. 8 Abs. 3 BV (Lohngleichheit zwischen Mann und Frau).<sup>373</sup> Auch SCHWEIZER bejaht die direkte Horizontalwirkung verschiedener Grundrechte, wenn sich eine privat- oder strafrechtliche Bestimmung als unvollständig oder verfas-

---

<sup>367</sup> SCHWEIZER, SG-Komm BV, N 48 zu Art. 35 BV; vgl. auch SCHEFER, Schutzpflichten, RZ 1138; BGE 126 II 300 ff. (314), E. 5a.

<sup>368</sup> SCHWEIZER, SG-Komm BV, N 49 zu Art. 35 BV; dabei ist mit SCHWEIZER einig zu gehen, dass der Begriff «Horizontalwirkung», wegen der Unterscheidung von vertikaler und horizontaler Dimension der Grundrechte besser passt, weshalb im Folgenden dieser Begriff verwendet wird.

<sup>369</sup> SCHWEIZER, SG-Komm BV, N 51 zu Art. 35 BV.

<sup>370</sup> SCHWEIZER, SG-Komm BV, N 58 zu Art. 35 BV; MAHON, N 10 zu Art. 35; RHINOW/SCHEFER, RZ 1171; MÜLLER JÖRG PAUL, Allgemeine Bemerkungen, N 37 zu Art. 39.

<sup>371</sup> BGE 118 Ia 46 ff. (56), E. 4c, BGE 114 Ia 329 (331), E 2b.

<sup>372</sup> BGE 120 V 312 ff. (316), E. 3b.

<sup>373</sup> BGE 120 V 312 ff. (316), E. 3b.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

sungswidrig erweist oder wo Grundrechtsgarantieren unmittelbar unter Privatpersonen Geltung beanspruchen.<sup>374</sup> Als explizit in der BV genannte Fälle direkter Horizontalwirkung nennt er u.a. Art. 118b Abs. 2 lit. a BV, wonach eine Person erst nach hinreichender Aufklärung ihre Einwilligung in ein Forschungsvorhaben erteilen kann und wonach eine Ablehnung in jedem Fall verbindlich ist, sowie Art. 119 Abs. 2 lit. g BV, der einer Person Anspruch auf Zugang zu den Daten ihrer Abstammung einräumt.<sup>375</sup>

Beim Erlass der zwischen Privaten geltenden Bestimmungen des DSG wurde ganz im Sinne der *Privatautonomie* davon ausgegangen, dass sich zwei ebenbürtige Subjekte gegenüberstehen.<sup>376</sup> Diese Annahme hat sich jedoch in Bezug auf Grossunternehmen, wie die vorne genannten, als falsch herausgestellt. Wie zu Beginn dieses Kapitels bereits erwähnt, haben solche Unternehmen ein enormes «Wissen»<sup>377</sup> über Individualpersonen, das sie letztlich häufig zu unbekannten und gegebenenfalls auch zu von den Betroffenen ungewollten Zwecken verwenden. Dieses «Wissen» übersteigt jenes, das Menschen normalerweise Fremden anvertrauen, um ein weites. Sich der Sammlung der eigenen Daten zu entziehen, ist hingegen fast unmöglich. Viele Anbieter gewähren ihre Dienstleistungen nur, wenn der einzelne bereit ist, seine Daten als Gegenleistung preiszugeben.<sup>378</sup> Die damit einhergehenden Gefahren für die freie Entwicklung selbstbestimmter Individuen wurden im Kapitel V auch deutlich beschrieben. Von einer Begegnung der Rechtssubjekte auf *Augenhöhe* kann

---

<sup>374</sup> SCHWEIZER, SG-Komm BV, 4, N 59 zu Art. 35 BV

<sup>375</sup> SCHWEIZER, SG-Komm BV, N 60 zu Art. 35 BV; wobei der hier vertretenen Auffassung nach zumindest dem Anspruch nach Art. 118b Abs. 2 lit. a BV mittlerweile durch die Schaffung einer formell-gesetzlicher Normierung im HFG Genüge getan wurde.

<sup>376</sup> Vgl. Botschaft DSG, S. 434.

<sup>377</sup> Meint hier «Besitzen von Informationen»; zum Umfang dieses «Wissen» siehe MAYER-SCHÖNBERGER/CUKIER, S. 15 ff..

<sup>378</sup> Zu denken ist hier an Rabatte, wenn man sich bereit erklärt, den Newsletter zu abonnieren, oder die Nutzung von «WhatsApp», welche die Übertragung des gesamten Adressbuches voraussetzt; Unbestrittenermassen werden zwar immer mehr datenschutzfreundliche Alternativen auf den Markt gebracht, vielfach sind deren Funktionen jedoch nicht mit dem Original zu vergleichen, was ihre Attraktivität schmälert. Hinzu kommt, dass solche Alternativen oft mit mehr Aufwand verbunden sind, weil der Dienst beispielsweise nicht schon auf dem Handy vorinstalliert ist oder weil es die Eingabe komplizierter Passwörter erfordert. Selbstverständlich bliebe immer noch die Möglichkeit, solche Dienste einfach nicht zu nutzen, aber gerade dies ist in der heutigen Zeit in unserer Gesellschaft eben keine echte Alternative mehr, weil ein Leben ohne Kreditkarte oder ohne solche Dienste wesentliche Einschränkungen im Alltag mit sich bringt.



## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

definitiv nicht mehr ausgegangen werden. In diesem Sinne kann bezüglich Unternehmen, die riesige Mengen von Daten von Personen sammeln, welche in keinerlei engeren Beziehung zu ihnen stehen und/oder diese Daten nicht zur Abwicklung einer konkreten Rechtsbeziehung zwischen ihnen und den Individualpersonen nutzen, sondern diese Daten für eigene Zwecke verwenden,<sup>379</sup> durchaus von einer *echten Lücke* im Privatrecht ausgegangen werden, was die Möglichkeit eröffnet, die direkte Horizontalwirkung für diesen Bereich zu bejahen.

Ob eine solche echte Lücke auch im Bereich ebenbürtiger Individuen angenommen werden darf, ist zu diskutieren. Obwohl grundsätzlich davon ausgegangen werden kann, dass von *Einzelpersonen* nicht die gleiche Gefährdung für die Privatheit zu erwarten ist wie durch oben beschriebene Unternehmen, so muss doch darauf hingewiesen werden, dass auch Einzelpersonen schon alleine aufgrund der durch die Digitalisierung geschaffenen Mittel der Datenbearbeitung in die Lage versetzt werden, erheblichen Schaden anzurichten. An dieser Stelle sei an das Beispiel des homosexuellen Hotelgastes erinnert, der aufgrund eines privaten Filmchens seine Stelle verloren hat.<sup>380</sup> Hier tritt denn auch unmittelbar die Frage zu Tage, ob das Individuum überhaupt die Verantwortung für die ihm durch die *Digitalisierung* zur Verfügung gestellten Mittel tragen kann. Obwohl die Frage aufgrund mangelndem Fachwissen in den einschlägigen Bereichen offen bleiben muss, wird für die vorliegende Arbeit davon ausgegangen, dass der einzelne zumindest einen Teil der Verantwortung zu übernehmen hat und der durch ihn verursachten Gefährdung für die Betroffenen u.a. deshalb grundsätzlich mittels grundrechtskonformen Gesetzen entgegengewirkt werden kann, was dem Ziel der indirekten Horizontalwirkung entspricht.<sup>381</sup> Dennoch sind auch zwischen ebenbürtigen Individuen Situationen denkbar, in denen der Gesetzgeber der informationellen Selbstbestimmung nicht zur Durchsetzung verhelfen kann und die sodann über den Weg der direkten Horizontalwirkung gelöst werden könnten (siehe dazu Kapitel VI, Ziffer 4.1.3).

---

<sup>379</sup> Dies im Gegensatz zu einem Grossunternehmen, das einfach deshalb viele Personendaten bearbeitet, weil es viele Angestellte hat und das diese Daten für die Abwicklung des Arbeitsverhältnisses braucht.

<sup>380</sup> Kapitel V, Ziffer 5.2.

<sup>381</sup> Zur möglichen gesetzgeberischen Anpassungen siehe Kapitel VI, Ziffer 4.

## 2.2 Indirekte Horizontalwirkung

Im Gegensatz zur direkten Horizontalwirkung von Grundrechten anerkennen die Lehre und auch das Bundesgericht mehrheitlich, dass Grundrechte zumindest indirekt auch zwischen Privaten gelten.<sup>382</sup> Art. 35 Abs. 3 BV normiert sodann eine Verpflichtung der Behörden, dafür Sorge zu tragen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Die indirekte Horizontalwirkung von Grundrechten bewirkt damit zweierlei: Einerseits muss der Gesetzgeber beim Erlass des Gesetzesrechts auf deren *grundrechtskonforme Ausgestaltung* achten, andererseits müssen rechtliche Erlasse *grundrechtskonform ausgelegt* werden.<sup>383</sup> Wie in Kapitel III, Ziffer 2.1 gezeigt wurde, sind, mit Blick auf das herrschende Verständnis der informationellen Selbstbestimmung, einige Lücken im Gesetzestext des DSG auszumachen. Vielfach hat allerdings der Gesetzgeber diese Lücken bewusst selbst geschaffen. So wurde beispielsweise bewusst normiert, dass die Informationspflicht nach Art. 14 DSG nur bei besonders schützenswerten Personendaten gilt. Aber auch das in Art. 12 Abs. 2 lit. b DSG angelegte Widerspruchsrecht sollte laut Botschaft bewusst nicht für jedes Datenbearbeiten Geltung beanspruchen können.<sup>384</sup> Es bestehen hier somit vor allem unechte Lücken, bei denen es zu überlegen gilt, ob sie nicht vom Gesetzgeber im Sinne der indirekten Horizontalwirkung nach dem herrschenden Verständnis der informationellen Selbstbestimmung gefüllt werden müssten.<sup>385</sup>

## 2.3 Fazit

Aufgrund dessen, dass die Gefahren für die Persönlichkeit des einzelnen und für das freiheitliche Gemeinwesen ganz allgemein nicht mehr nur vom Staat ausgehen, son-

---

<sup>382</sup> SCHWEIZER, SG-Komm BV, N 55 zu Art. 35 BV; BGE 130 III 28 ff. (32), E. 4.2, worin das Bundesgericht drauf hinweist, dass die Grundrechte Richtschnur dafür sein können, was unter Privaten tolerierbar ist.

<sup>383</sup> SCHWEIZER, SG-Komm BV, N 56 zu Art. 35 BV.

<sup>384</sup> Botschaft DSG, S. 459.

<sup>385</sup> Ganz in diesem Sinne vertritt auch SCHWEIZER die Auffassung, dass die indirekte Horizontalwirkung mit zunehmender privater Aneignung sicherheitspolitischer Befugnisse, wie beispielsweise die private Videoüberwachung öffentlich zugänglicher Räume, immer wichtiger wird (SCHWEIZER, SG-Komm BV, N 56 zu Art. 35 BV).

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

dern auch von privaten Unternehmen, welche unvorstellbare Mengen von Personendaten sammeln, die sie nicht zur Abwicklung einer konkreten Rechtsbeziehung zwischen ihnen und den betroffenen Individualpersonen beanspruchen, könnte für solche Unternehmen eine direkte Horizontalwirkung der informationellen Selbstbestimmung bejaht werden. Damit würde eine unmittelbare Bindung solcher Unternehmen an das Grundrecht begründet und dessen Wirkungskreis vergrößert.

In Bezug auf die übrigen privatrechtlichen Unternehmen und Einzelpersonen ist von einer indirekten Horizontalwirkung der informationellen Selbstbestimmung auszugehen, welche den Gesetzgeber verpflichtet, insbesondere die grundlegenden Bestimmungen des DSG an das herrschende Verständnis des Grundrechts anzupassen, um ihm dadurch vermehrte Durchsetzungskraft zu verschaffen (siehe dazu Kapitel VI, Ziffer 4.1).

### 3 Parallelen zu anderen Rechten

#### 3.1 *Annäherung an das sachenrechtliche Eigentum*

In den USA wird schon seit einiger Zeit dafür plädiert, das Recht an den eigenen Daten als Eigentumsrecht auszugestalten. So proklamiert beispielsweise WESTIN: «personal information, thought of as the right of decision over one's personality should be defined as a property right.»<sup>386</sup> Dahinter steckt die Idee, dass mit dem Zugeständnis eines Eigentumsrechts an persönlichen Daten der einzelne mehr Macht bezüglich deren Verwendung erhält und er so seine Persönlichkeit besser zu schützen vermag.

##### 3.1.1 **Ausdehnung des Sachbegriffs**

Auch einige Schweizer Autoren sind zur Ansicht gelangt, dass die sachenrechtlichen Bestimmungen bezüglich des Eigentumsrechts sowie im Hinblick auf weitere beschränkte dingliche Rechte auf persönliche Daten Anwendung finden sollten.<sup>387</sup>

---

<sup>386</sup> WESTIN, S. 7.

<sup>387</sup> FLÜCKIGER, S. 32; HESS-ODONI, RZ 54; MONNIER sieht den Datenschutz gar als Mittelweg zwischen den dinglichen Rechten und den Persönlichkeitsrechten: «Le droit de la protection des données et la notion de maîtrise développée à cet égard trouvent effectivement très bien leur place entre

HESS-ODONI hat auf verschiedenste Weise versucht, sachenrechtliche Herrschaftsrechte an Daten herzuleiten. Zu diesem Zweck hat er als erstes geprüft, ob sich nicht der Sachbegriff modifizieren lasse, da das ZGB diesen zwar umschreibt, aber nicht mittels einer Legaldefinition an die Körperlichkeit bindet. Ein solcher teleologischer Ansatz ist seiner Meinung nach gerechtfertigt, da bei der rechtlichen Qualifikation eines Gegenstandes als Sache neben den physikalischen Eigenschaften auch wirtschaftliche, praktische und ethische Gesichtspunkte eine Rolle spielen würden.<sup>388</sup> In diesem Zusammenhang muss erwähnt werden, dass es durchaus beschränkte dingliche Rechte gibt, die auch auf nichtkörperliche Gegenstände Anwendung finden, wie beispielsweise das Pfandrecht an Forderungen.<sup>389</sup> HESS-ODONI verwirft die Möglichkeit der Ausdehnung des Sachbegriffs jedoch, da der historische Gesetzgeber offensichtlich nur körperliche Gegenstände als Sachen bezeichnen wollte und diese historische Argumentation durch die herrschende Lehre und Rechtsprechung immer und ohne relevanten Widerspruch gestützt worden sei. Darüber hinaus gebe es im Sachenrecht zahlreiche Bestimmungen, die nur auf körperliche Gegenstände richtig passen würden.<sup>390</sup> Unter diesen Umständen liegt nach HESS-ODONI eine *echte Gesetzeslücke* vor, welche im Sinne von Art. 1 Abs. 2 ZGB zu schliessen sei. Da sich das Schweigen des Gesetzgebers unzweifelhaft mit einer historisch bedingten Unkenntnis erklären lasse, könne ein qualifiziertes Schweigen ausserdem klar ausgeschlossen werden.<sup>391</sup> In seinen weiteren Ausführungen verzichtet er jedoch darauf, eine generelle Regel für einen sachverwandten Umgang mit Daten aufzustellen, sondern prüft für jeden Bereich der möglichen Herrschaftsrechte gesondert, ob eine analoge Behandlung der Daten mit beweglichen Sachen möglich und sinnvoll ist.<sup>392</sup> Er kommt zum Schluss, dass – abgesehen von den Besitzesregeln – absolute und beschränkte Herrschaftsrechte an Daten begründet werden können, die grosse Ähnlichkeit mit den entsprechenden Rechten an Sachen im Sinne des ZGB haben.<sup>393</sup>

---

les droits réels (maîtrise au sens de possession) et la protection de la personnalité (maîtrise au sens de droit de la personnalité)». (MONNIER, S. 143, FN 18); vgl. auch SCHWARZ, S. 19.

<sup>388</sup> HESS-ODONI, RZ 22 ff.

<sup>389</sup> ERNST, S. 20.

<sup>390</sup> HESS-ODONI, RZ 27.

<sup>391</sup> HESS-ODONI, RZ 34 f.

<sup>392</sup> HESS-ODONI, RZ 37 ff.

<sup>393</sup> HESS-ODONI, RZ 54.

Leider geht HESS-ODONI hier zu wenig auf die datenspezifischen Eigenheiten wie die uneingeschränkte Reproduzierbarkeit und Verteilbarkeit oder die Schwierigkeit, dass ein Datum gleichzeitig mehrere Personen identifizieren kann, ein, weshalb nicht von einem eigenen Ansatz gesprochen werden kann.

### 3.1.2 Analoge Anwendbarkeit

Die der informationellen Selbstbestimmung zugrunde liegende Idee eines Dispositionsrechts über die eigenen Daten weist tatsächlich erhebliche Ähnlichkeiten zum Eigentum auf. Die analoge Anwendbarkeit der sachenrechtlichen Regeln bezüglich des Eigentums würde allerdings voraussetzen, dass es sich bei persönlichen Daten um sachähnliche Dinge handelt. Das ZGB definiert zwar den Begriff der Sache nicht, es stellt aber fest, dass Grundstücke Gegenstand des Grundeigentums und die «ih-  
rer Natur nach beweglichen körperlichen Sachen» als Gegenstand des Fahrniseigen-  
tums zu gelten haben.<sup>394</sup> Nach Lehre und Rechtsprechung wird eine *Sache* im Sinne  
des ZGB deshalb auch als ein unpersönlicher (im Sinne von vom menschlichen Kör-  
per verschiedener), räumlich begrenzter, körperlicher Gegenstand, der eine gewisse  
Zeit Bestand hat und der menschlichen Herrschaft unterworfen werden kann, defi-  
niert.<sup>395</sup> Solange Informationen in einem Foto, Buch etc. manifestiert sind, können die  
Daten, wie im Kapitel IV, Ziffer 6.3 dargestellt, sehr wohl als Sachen im sachenrecht-  
lichen Sinne angesehen werden. Nichtmanifestierte Information oder digitalisierte  
Daten sind hingegen gerade das Gegenteil einer Sache. Zwar können *digitalisierte  
Daten* ebenso wie «handfeste» Daten als unpersönlich bezeichnet werden, auch  
kann die Beherrschbarkeit im dem Sinne, dass die Sache erworben, veräußert oder  
genutzt werden kann, bejaht werden, da es durchaus möglich ist, auch nichtmanifes-  
tierte Daten oder Informationen weiterzugeben, zu vernichten oder zu neuen digita-  
len, aber auch manifestierten Daten zusammenfügen. Jedoch bereitet bereits die  
weitere Voraussetzung der *Körperlichkeit* Probleme: Die uns z.B. auf dem Bildschirm  
erscheinenden digitalen Daten sind nicht greifbar, also nicht körperlich, höchstens  
der Bildschirm selbst kann angefasst werden, die darauf zu erblickenden Daten tre-  
ten nur als zweidimensionale Erscheinungen auf. Die Körperlichkeit rückt noch mehr

---

<sup>394</sup> Art. 655 und 713 ZGB.

<sup>395</sup> HESS-ODONI, S. 2; SCHMID/HÜRLIMANN/KAUP, RZ 4 ff.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

in die Ferne, wenn es sich um digitale Tondaten handelt, also um rein akustisch wahrnehmbare Aufnahmen, die wir von unseren Computer abspielen oder eben auch unbegrenzt weiterverbreiten etc. können. Die Anmerkung von DRUEY, dass gerade die *unbegrenzte Verteilbarkeit* der Information auf die Unmöglichkeit einer Sachanalogie hinweisen würde,<sup>396</sup> betrifft jedoch in erster Linie die Verfügbarkeit der Information als solche und nicht deren Einordnung als Sache. Dem von DRUEY gewählten Ansatz liegt die Annahme zugrunde, dass, wenn eine Sache unbeschränkt verteilbar ist, keiner der sie besitzenden Personen alleine darüber disponieren kann und somit einen Anspruch auf das alleinige Entscheidungsrecht darüber geltend machen könnte, was die grundsätzliche Idee einer Sache ist. Jedoch sind auch Immaterialgüter unbeschränkt verteilbar, und dennoch sieht das Gesetz eine Sachanalogie vor. Die Frage der Verteilbarkeit ist somit nicht eine Frage der Sachanalogie, sondern der Verfügbarkeit und, es wird zu zeigen sein, dass letztere nicht der einzige Anhaltspunkt sein muss, um eine Entscheidungsbefugnis zu rechtfertigen. Auch die für die erga omnes wirkende Zuordnung erforderliche Erkennbarkeit der Beziehung nach aussen betrifft das Recht an der Sache, also die Entscheidungsbefugnis darüber, und nicht die Sache selbst. Eine Sache ist eine Sache, auch wenn niemand das Recht an ihr hat, dann ist sie halt eine herrenlose Sache, aber sie bleibt eine Sache und aufgrund dessen kann an ihr Eigentum, sprich das Verfügungs- oder besser das Entscheidungsrecht über sie, erworben werden. In diesem Zusammenhang wird auch die Meinung vertreten, dass zwischen Daten auf Datenträgern und *Wertpapieren*, welche Rechte verbriefen und insofern verkörpern, eine gewisse Ähnlichkeit festgestellt werden kann. Das Wertpapier als Papier sei ebenso wie beispielsweise das Fotoalbum zweifellos eine Sache, aber eben nur Medium, um das eigentlich Wichtige, nämlich die Rechte oder die Daten, festzuhalten.<sup>397</sup> Dieser Ansatz ist interessant, hilft jedoch auch nur bedingt weiter, da der Gesetzgeber im Bundesgesetz über Bucheffekten die elektronisch verwahrten Bucheffekten entkörperlicht hat, indem er darin die Zuordnungsregeln von jenen des Sachenrechts nach ZGB verschieden geregelt hat.<sup>398</sup> Auch ein Analogieschluss zu den *Naturkräften*, welche vom ZGB trotz ihrer mangelnden Körperlichkeit auch als Gegenstand des Fahrniseigen-

---

<sup>396</sup> DRUEY, Information, S. 33.

<sup>397</sup> ERNST, S. 15.

<sup>398</sup> ERNST, S. 15.

tums bezeichnet werden, wenn sie eben der rechtlichen Herrschaft unterworfen werden können und nicht zu den Grundstücken gehören (Art. 713 ZGB), muss verneint werden. Der Vergleich zwischen Daten und Naturkräften hinkt, da Daten bereits von ihrer Art her nicht mit Naturkräften verglichen werden können, da erstere individuell fixiert sind, sich beliebig vervielfältigen und weiterbearbeiten lassen, ohne dass sie dabei ihre ursprünglichen Entitäten verlieren müssten, was bei Naturkräften nicht der Fall ist.<sup>399</sup> Darüber hinaus handelt es sich bei den Naturkräften um eine explizite Ausnahmeregelung und es wird betont, dass die Ausdehnung des Sachbegriffs auf die Energie nur beschränkt und sinngemäss erfolgen könne.<sup>400</sup>

### 3.1.3 Fazit

Aufgrund der fehlenden Körperlichkeit von Informationen und Daten erweisen sich die Versuche, den Sachbegriff auszudehnen oder eine Analogie zur Sache herzustellen, als missglückt. Ganz generell sieht MAYER-SCHÖNBERGER Probleme bei der Annäherung der Selbstbestimmung bezüglich der eigenen Daten an das sachenrechtliche Eigentum, da die Beziehung zwischen Mensch und Information eben nicht nur eindimensional verlaufe. Zwar könne jede Beziehung zwischen Information und Mensch als Subjekt-Objekt-Relation eine eigentumsähnliche Struktur aufweisen, indem der einzelne über die ihm zuzurechnende Information disponieren könne, ganz so als wäre sie sein Eigentum. Gleichzeitig sei aber jede Information von einem Menschen auch eine über ihn. In ihr spiegle sich ein besonderer Aspekt seiner Identität, seiner selbst wider. Ihre Richtung sei der eigentumsähnlichen Relation entgegengesetzt, sie zeige von der Information zum Menschen – vom Abbild zum Original.<sup>401</sup> Auch BELSER stellt sich die Frage, ob die Anerkennung eines eigentumsähnlichen Verfügungsrechts im Bereich der Personendaten geeignet ist, die Gefahren moderner Datenbearbeitung einzudämmen, oder ob dieses nicht vielmehr zu einer kaum zu überbrückenden Kluft zwischen rechtlichem Anspruch und Wirklichkeit führt». <sup>402</sup>

---

<sup>399</sup> HESS-ODONI, RZ 11.

<sup>400</sup> HESS-ODONI, RZ 30, mit Verweis auf HAAB/SIMONIUS/SCHERRER/ZOBL, N 46 der Einleitung.

<sup>401</sup> MAYER-SCHÖNBERGER, S. 42.

<sup>402</sup> BELSER, Instrumente, S. 25.

### 3.2 *Daten als Immaterialgüter*

FLÜCKIGER plädiert in Anlehnung an HESS-ODONI ebenfalls dafür, dass die sachenrechtlichen Bestimmungen *mutatis mutandis* auf persönliche Daten angewendet werden sollen. Allerdings sieht er vor allem Ähnlichkeiten zu den Rechten des geistigen Eigentums oder – wie sie in der Schweiz genannt werden – den Immaterialgüterrechten: «L'exemple du droit à son propre image, tantôt protégé par le droit d'auteur, tantôt par le droit de la personnalité et de la protection des données, montre pourtant que l'assimilation de cette dernière avec la propriété intellectuelle est une piste stimulante pour repenser tout le droit de la protection des données dans le monde numérique.»<sup>403</sup> Auch DESSEMONTET möchte das Recht am eigenen Bild, welches zweifellos ein Personendatum darstellt, als Immaterialgut einordnen.<sup>404</sup>

#### 3.2.1 Definition und Gemeinsamkeiten

Bei Immaterialgütern handelt es sich um *geistige Schöpfungen*, die aufgrund ihrer *wirtschaftlichen Bedeutung* von der Rechtsordnung einem besonderen Schutz unterstellt sind, welcher dem sachenrechtlichen Eigentum möglichst nahe kommen soll.<sup>405</sup> Wie das Eigentum gewähren diese Rechte ihrem Inhaber die ausschliessliche Befugnis, die geschützten Güter wirtschaftlich zu verwerten sowie gegenüber jedermann vorzugehen, der ohne Erlaubnis vom Rechtsinhaber das geistige Gut gebraucht, und diesen Gebrauch zu verbieten.<sup>406</sup>

Eine den Immaterialgütern analoge Behandlung persönlicher Daten scheint zumindest auf den ersten Blick gar nicht so weit hergeholt, da sich diese in ähnlicher Weise wie die Immaterialgüter von Sachen im Sinne des ZGB unterscheiden. Als erste Gemeinsamkeit ist die *Unerschöpflichkeit* vom Zeitpunkt der Schaffung an zu nennen. Immaterialgüter sind gleich wie digitale Daten kostenlos reproduzierbar. Kosten fallen allenfalls durch notwendige materielle Träger wie Papier oder dergleichen an. Als

---

<sup>403</sup> FLÜCKIGER, S. 33.

<sup>404</sup> «La reconnaissance d'un droit patrimonial à l'image permet de tirer une distinction plus nette entre les intérêts personnels réels – toujours protégés au titre de l'article 28 CC – et les intérêts commerciaux» (DESSEMONTET, S. 52).

<sup>405</sup> KAISER/RÜETSCHI, S. 1.

<sup>406</sup> KAISER/RÜETSCHI, S. 3.



zweite gemeinsame Eigenschaft fehlt es solchen immateriellen Gütern wie den digitalen Daten an der Möglichkeit des *faktischen Ausschlusses Dritter*. Sobald das Immaterialgut öffentlich ist, kann es von jedermann genutzt werden, ohne dass sich der Schöpfer mit faktischen Mitteln dagegen wehren kann.<sup>407</sup>

### 3.2.2 Analoge Anwendbarkeit des URG?

Das Immaterialgüterrecht schützt verschiedene immaterielle Güter mit verschiedenen Rechten, wobei ein *numerus clausus* geschützter Immaterialgüterrechte besteht.<sup>408</sup> Dabei werden die folgenden Immaterialgüterrechte anerkannt: Das *Urheberrecht* (engl. Copyright), welches den Schutz von Werken der Literatur und Kunst sicherstellt, das *Patentrecht*, welches den Erfindungsschutz gewährleistet, das *Markenrecht*, welches Kennzeichen schützt, sowie *Designrechte*, *Rechte an Topographien von Halbleiterzeugnissen* und *Sortenschutzrechte*.<sup>409</sup>

Nach FLÜCKIGER ist die Konstruktion eines Eigentumsrechts an persönlichen Daten nicht sehr weit entfernt von den Prinzipien des Urheberrechts.<sup>410</sup> Durch die Anwendung der urheberrechtlichen Bestimmungen auf persönliche Daten verspricht er sich die Stärkung einer Art Gegenmacht des Dateneigentümers. Dieser könne dann nicht nur den materiellen Gegenwert für die Verwendung seiner Daten aushandeln, er könne auch über die Verwendung selbst bestimmen.<sup>411</sup> Ökonomen wie APERJIS/HUBERMAN haben sogar bereits begonnen, diese Idee als neuen Geschäftszweig für sich zu sehen: «Since there is, in principle, no reason why third parties should not pay individuals for the use of their data, we introduce a realistic market that would allow these payments to be made while taking into account the privacy attitude of the participants.»<sup>412</sup>

---

<sup>407</sup> KAISER/RÜETSCHI, S. 2.

<sup>408</sup> KAISER/RÜETSCHI, S. 1.

<sup>409</sup> KAISER/RÜETSCHI, S. 1 f.

<sup>410</sup> FLÜCKIGER, S. 35.

<sup>411</sup> FLÜCKIGER, S. 36 f.; vgl. in diesem Zusammenhang auch das Geschäftsmodell von «patrimoine-immateriel.fr», welche verschiedene Arten Lizenzen vergibt, mit denen man einen Dritten autorisieren kann, die eigenen Daten oder nur einen Teil davon weiter zu verwenden.

<sup>412</sup> APERJIS/HUBERMAN, S. 1.

### 3.2.2.1 Der Werkbegriff

Damit der Urheberrechtsschutz zum Tragen kommt, muss es sich bei Daten allerdings um ein Werk im Sinne des URG handeln und es darf nicht durch Art. 5 URG vom Urheberrechtsschutz ausgeschlossen sein. Werke im Sinne des URG sind definiert als *geistige Schöpfungen* der Literatur und Kunst, die einen *individuellen Charakter* haben, ausserdem Werke zweiter Hand und Sammelwerke. Als Werke gelten nach Art. 2 Abs. 3 URG auch Computerprogramme. Laut Bundesgericht handelt es sich dann um eine «geistige Schöpfung», wenn ein Werk auf menschlichem Willen beruht und Ausdruck einer Gedankenäusserung ist.<sup>413</sup> Letzteres ist dann gegeben, wenn sich die Gedankenäusserung in einer durch die Sinne wahrnehmbaren Form materialisiert hat. Geschützt ist also nicht die Idee, sondern der sinnlich wahrnehmbare Ausdruck dieser Idee.<sup>414</sup> Dies bedeutet: Geschützt ist jeweils nur der konkrete Roman, das konkrete Bild, nicht aber das abstrakte Konzept, das dahinter steckt.<sup>415</sup> Dementsprechend halten die Amerikaner auch fest: «Copyright protects expressions, not ideas.»<sup>416</sup> In Bezug auf die personenbezogenen Daten bedeutet dies, dass zwar das analoge oder digitale Datum geschützt ist, nicht jedoch die daraus entnehmbare Information. Dies dürfte aber hinsichtlich des verfolgten Schutzzwecks der informationellen Selbstbestimmung nicht aufgehen, da die Daten nicht um ihrer selbst willen geschützt werden, sondern hinsichtlich ihres Informationsgehalts zu einer bestimmten Person. Wie MAYER-SCHÖNBERGER dies bezüglich des Datums des Namens formuliert hat: «Geschützt ist daher die Buchstabenkombination des Namens selbst nur mittelbar, direkt jedoch die Verknüpfung der Buchstabenfolge mit einer individuellen Person, deren Identität sich auch auf diesen Namen gründet.»<sup>417</sup> Entsprechend ist der Meinung von BEUTHIEN nur teilweise zu entsprechen, wenn er festhält, dass nicht die Persönlichkeit oder die sie prägenden Persönlichkeitsmerkmale vermarktet werden, sondern ihr gesellschaftlicher Abdruck. Und da sich dieser ausserhalb der Per-

---

<sup>413</sup> BGE 130 III 168 ff. (172 f), E. 4.5.; um keine geistige Schöpfung handelt es sich deshalb bei Dingen, die natürlich entstehen oder die durch eine Maschine automatisch geschaffen wurden. Allerdings ist der Urheberrechtsschutz bei letzterem möglich, wenn die Maschine die schöpferische Tätigkeit eines Menschen ersetzt (KAISER/RÜETSCHI, S. 30).

<sup>414</sup> KAISER/RÜETSCHI, S. 30 f.

<sup>415</sup> KAISER/RÜETSCHI, S. 10.

<sup>416</sup> KAISER/RÜETSCHI, S. 10.

<sup>417</sup> MAYER-SCHÖNBERGER, S. 33.

son befinde, lasse er sich als immaterieller Gegenstand und damit als Immaterialgut begreifen.<sup>418</sup> Oder, wie es LESSIG formulierte: «The problems of privacy and copyright are exactly the same. With both, there's a bit of ,our' data that ,we've' lost control over.»<sup>419</sup>

Bezüglich der für die geistige Schöpfung notwendigen Voraussetzung des *menschlichen Willens* lässt sich festhalten, dass personenbezogene Daten nicht «einfach so» entstehen. Wie die Definition im Kapitel IV, Ziffer 6.3 zeigt, handelt es sich bei Daten um die Manifestation von Informationen und diese stellen das Resultat menschlicher Gedanken dar. Selbst wenn der Computer neue Daten durch das Zusammenführen anderer Daten entstehen lässt, tut er dies auf menschlichen Befehl hin und mit der Absicht, bestimmte weitere Personendaten zu erhalten. Würde der Computer die Daten nicht zu neuen Daten zusammenfügen, würde es ein Mensch tun, da der Computer keiner personenbezogenen Daten für sein Funktionieren im Sinne eines Selbstzwecks bedarf und somit auch nicht generiert. Der Computer ersetzt beim Zusammenfügen bestehender Daten zu neuen Daten also die schöpferische Tätigkeit des Menschen, auch wenn ein solcher zugegebenermassen sehr lange hätte, um die gleiche Arbeit auszuführen.

Betrachtet man allerdings das Phänomen «big data», so gelangt diese Auffassung bereits wieder ins Wanken. Durch das Zusammenführen riesiger Datenmengen können Prognosen bezüglich des einzelnen Menschen erstellt werden, die dann mit grösserer oder kleinerer Wahrscheinlichkeit eintreffen werden.<sup>420</sup> Die Programmierung für das Zusammenfügen der Daten findet zwar auch wieder durch den Menschen statt, allerdings hat dieser zum Zeitpunkt des Programmierens keinerlei Ahnung, welche Daten dabei herauskommen werden, insoweit der menschliche Wille in Bezug auf die produzierten Daten und damit die geistige Schöpfung für solche Daten zu verneinen ist.<sup>421</sup>

---

<sup>418</sup> BEUTHIEN, Persönlichkeitsrecht, S. 77.

<sup>419</sup> LESSIG, S. 200 mit Verweis auf ZITTRAIN.

<sup>420</sup> Vgl. POLZER, S. 9; vgl. zur Problematik «big data» Kapitel V, Ziffer 7.

<sup>421</sup> Vgl. BURKERT, S. 4.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

Das zweite Definitionsmerkmal für den Werkbegriff, der individuelle Charakter, wird vom Bundesgericht mit «der Notwendigkeit einer statistischen Einmaligkeit» umschrieben.<sup>422</sup> Dabei wird das Werk mit dem verglichen, was andere bei gleicher Aufgabenstellung geschaffen haben oder schaffen könnten. Verlangt wird also de facto «ein gewisser kreativer Abstand gegenüber dem Üblichen und in Zukunft zu Erwartenden».<sup>423</sup> Objektive Neuheit wird demgegenüber nicht verlangt. Vorausgesetzt, es handelt sich um eine unabhängige Schöpfung, sind damit auch sog. Doppelschöpfungen möglich und urheberrechtlich schützbar.<sup>424</sup> Dies stellt aber gerade in Bezug auf persönliche Daten ein Problem dar. So könnte beispielsweise ein Foto einer Person in ein anderes Bild eingefügt werden und dieses neue Bild könnte dann als eigene Schöpfung vom Urheberrecht geschützt werden, obwohl die betroffene Person vielleicht nicht einmal weiss, dass ihr Bild neu verarbeitet wird, geschweige denn dazu eingewilligt hat. Es ergeben sich aber noch weitere *Schwierigkeiten*, wenn Daten unter den Urheberrechtsschutz gestellt werden könnten: Unabhängig von der konkreten Art der Weiterverbreitung solcher Werke handelt es sich dabei immer um die Herstellung von *Kopien* vorhandener Werkexemplare, was nach Art. 10 Abs. 2 lit. a URG eine dem Rechtsinhaber vorbehaltene Verwertungshandlung darstellt.<sup>425</sup> Das Kopieren und die Weitergabe von digitaler Musik und digitalen Filmen (egal ob via Datenträger oder übers Internet) *zum Eigengebrauch* im persönlichen Bereich ist allerdings zulässig, ohne dass eine Vergütung geschuldet ist.<sup>426</sup> Unzulässig ist einzig das Zuverfügungstellen von geschützten Werken im Internet für einen nicht persönlich bekannten oder einen nicht mehr kontrollierbaren Personenkreis und dies unabhängig davon, ob damit eine Gewinnerzielung bezweckt wird oder nicht.<sup>427</sup> Ob dann auch das Herunterladen von geschützten Werken aus dem Internet ohne Erlaubnis des Rechteinhabers erlaubt ist oder nicht, ist derzeit umstritten.<sup>428</sup> Ferner bezieht sich bei Daten der Schutz im Gegensatz zu Werken wie Büchern, Musik etc. nicht darauf, dass der Urheber eine für seine geleistete Arbeit angemessene Entschädigung er-

---

<sup>422</sup> BGE 130 III 168 ff. (171 f.), E. 4.5.

<sup>423</sup> KAISER/RÜETSCHI, S. 33.

<sup>424</sup> KAISER/RÜETSCHI, S. 33.

<sup>425</sup> KAISER/RÜETSCHI, S. 51 f.

<sup>426</sup> KAISER/RÜETSCHI, S. 52.

<sup>427</sup> KAISER/RÜETSCHI, S. 52.

<sup>428</sup> KAISER/RÜETSCHI, S. 52.

hält. Der Schutzzweck der Selbstbestimmung bezüglich des Umgangs mit persönlichen Daten ist – gleichgültig, welcher Lehrmeinung gefolgt wird – auf jeden Fall nicht finanzieller Natur. Vielmehr geht es um den Schutz eines persönlichen Gutes, ähnlich wie beim Recht am eigenen Bild. Ähnlich sahen dies WARREN/BRANDEIS: Ihrer Meinung nach handelt es sich beim Prinzip, welches persönliche Schriften und andere persönliche Produktionen vor fremder Publikation schützt, nicht um das des Eigentums, sondern um das einer unverletzten Persönlichkeit. «The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in a form, is in reality not the principle of private property, but that of an inviolate personality.»<sup>429</sup>

### **3.3 Fazit und Überleitung**

Die dargestellten Versuche, Analogien zum sachenrechtlichen Eigentum oder zum Immaterialgüterrecht, konkret zum Urheberrecht, zu finden, um dem Recht auf informationelle Selbstbestimmung dadurch zu mehr «Griffigkeit» zu verhelfen, überzeugen nicht recht. Obwohl die hinter dem Recht auf informationelle Selbstbestimmung stehende Idee einer Dispositionsfreiheit klar am sachenrechtlichen Eigentum orientiert ist, kann eine Analogie aufgrund der fehlenden Körperlichkeit von Informationen und digitalen Daten nicht hergestellt werden. Mit den Immaterialgütern gibt es zwar gerade in dieser Hinsicht Ähnlichkeiten, doch verfolgen sie einen derart anderen Schutzzweck, dass sich die Bestimmungen nicht zur analogen Anwendung auf Daten und Informationen eignen. Dies bedeutet nicht, dass die dargestellten Ansätze komplett zu verwerfen wären. Sie könnten allenfalls im Kontext der Überlegungen zu einem gänzlich neuen Recht zusammengefügt werden.<sup>430</sup>

---

<sup>429</sup> WARREN/BRANDEIS, S. 205.

<sup>430</sup> Zum Beispiel im Sinne des amerikanischen Right of Publicity, welches als selbstständiges intellectual property law angesehen wird (siehe MEYER, RZ 200).

## 4 Revision und Interpretation DSG sowie Kompetenzerweiterung des EDÖB

### 4.1 Revision DSG

#### 4.1.1 Paradigmawechsel mit Revision von Art. 12 DSG

Wie bereits an anderer Stelle erläutert (Kapitel III, Ziffer 2.1), setzt das DSG die Idee eines informationellen Selbstbestimmungsrechts nicht konsequent um. Eine Bestimmung, die diese Aussage am besten untermauert, ist Art. 12 Abs. 2 lit. b DSG, wonach private Datenbearbeiter die betroffenen Personen nicht anfragen müssen, ob sie mit der durch sie erfolgten Datenbearbeitung einverstanden sind, was bedeutet, dass die Bearbeitung von Personendaten grundsätzlich ohne Einwilligung der betroffenen Person zulässig ist.<sup>431</sup> Nach dem derzeitigen Gesetzeswortlaut ist es vielmehr an der betroffenen Person selbst, sich *ausdrücklich* gegen eine Datenbearbeitung durch Private auszusprechen. Dies bedeutet, dass sie gegenüber einer bestimmten Person, bezogen auf bestimmte Daten und Datenbearbeitungen das *Widerspruchsrecht* ausüben muss und dazu noch die Beweislast für die Ausübung trägt.<sup>432</sup> Möchte man der informationellen Selbstbestimmung aufgrund des ausgewiesenen Schutzbedarfs<sup>433</sup> jedoch zum Durchbruch im Sinne ihrer indirekten Horizontalwirkung verhelfen, müssten Art. 12 DSG sowie die auf diesem Verständnis aufbauenden Artikel dahingehend revidiert werden, dass, wer als *Privatperson* Personendaten oder Informationen, die einen Personenbezug aufweisen, bearbeiten möchte und dies eben nicht zum persönlichen Gebrauch tut oder/und die Absicht hat, die Daten/Informationen an Aussenstehende bekannt zu geben, grundsätzlich die betroffene Person um Einwilligung ersuchen muss.<sup>434</sup> Natürlich würde durch eine solche Neukonzeption die Bindung an die allgemeinen Grundsätze von Art. 4, 5 Abs. 1 und 7 Abs. 1 DSG nicht ausgehebelt, ebenso wenig würde sie den bestehenden Rechtfertigungsgründen (überwiegendes privates oder öffentliches Interesse

---

<sup>431</sup> RAMPINI, BaKomm DSG, N 12 zu Art. 12 DSG; ROSENTHAL, Handkommentar DSG, N 26 zu Art. 12.

<sup>432</sup> RAMPINI, BaKomm DSG, N 10 zu Art. 12 DSG; siehe zu den Problemen dieser Widerspruchslösung Kapitel III, Ziffer 2.1.

<sup>433</sup> Zur Schutzbedarfsanalyse siehe Kapitel V.

<sup>434</sup> Vgl. ROSENTHAL, Handkommentar DSG, N 26 zu Art. 12.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

sowie Gesetz) entgegenstehen. Ein Arbeitnehmer kann dem Arbeitgeber etwa nicht verbieten, Personendaten, welche er zur Abwicklung des Arbeitsverhältnisses bedarf, zu bearbeiten. Auch an der in Art. 12 Abs. 3 DSG vorgesehenen Ausnahme, wonach es keiner Einwilligung bedarf, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat und der Bearbeitung nicht widersprochen hat, müsste festgehalten werden. Neu wären jedoch die Situationen zu regeln, wenn ein Personendatum sich auf mehrere Personen bezieht und nicht alle ihre Einwilligung in die Datenbearbeitung geben oder/und wenn es sich als unverhältnismässig schwierig erweist, die Einwilligung der Betroffenen einzuholen (dazu sogleich Kapitel VI, Ziffer 4.2).

Diese sog. *opt-in-Lösung* mag als informationsfeindlich angesehen werden. Es ist sich allerdings zu vergegenwärtigen, dass es sich dabei nicht um die Erfüllung einer staatlichen Aufgabe handelt, sondern dass es um Situationen geht, in denen Privatpersonen ohne Rechtfertigungsgrund persönliche Daten über andere (und nicht etwa Sachdaten) zu einem *eigenen* Zweck bearbeiten möchten. Personendaten sind für gewöhnlich kein Kulturgut, zumindest nicht, wenn man sich die aus einer eben solchen Überzeugung resultierenden Phänomene wie «big data» und die damit einhergehenden Gefahren für die Entwicklung selbstbestimmter Individuen vor Augen hält. Jene Fälle, die aufgrund überwiegender öffentlicher Interesse anders beurteilt werden müssen, wie Forschung, Planung oder Vertragsabwicklung, sind vom Gesetzgeber deutlich als Ausnahmen zu deklarieren, wie er dies bereits heute in Art. 13 DSG getan hat. Weshalb gerade im Bereich der privaten Datenbearbeitung der allgemeine Grundsatz, wonach derjenige, der etwas vom anderen will, diesen darum bitten muss, und es sich nicht einfach nehmen kann, nicht angewendet werden soll, ist nicht nachvollziehbar.<sup>435</sup>

---

<sup>435</sup> In diesem Kontext ist sich zu vergegenwärtigen, dass sich die traditionelle Sicht der Verhältnisse Staat-Bürger und Bürger-Bürger gewandelt haben und sich mittlerweile eigentlich nur Anbieter und Kunden gegenüberstehen, seien die Leistungen privater oder öffentlicher Natur. Dies hat zur Folge, dass sich das Individuum mittlerweile mit beiden «Mächten» in ähnlich zwanghafter Weise konfrontiert sieht (vgl. GARSTKA, S. 162 f.) und sich ganz grundsätzlich die Frage nach der Zulässigkeit bzw. Zumutbarkeit der Einwilligung im staatlichen, aber eben auch im privatrechtlichen Kontext stellt, sofern ähnliche Machtverhältnisse vorliegen (vgl. KAMP/ROST, S. 80 ff. und GÄCHTER/WERDER, S. 95 ff.).

#### 4.1.2 Revision Art. 3 lit. a DSG

Wie gezeigt wurde, geht nicht nur vom Umgang mit personenbezogenen Daten eine Gefahr für die Persönlichkeit der Betroffenen aus, sondern auch vom Umgang mit personenbezogenen Informationen. Das DSG ist jedoch nur anwendbar auf die Bearbeitung von Personendaten (Art. 2 Abs. 1 DSG). Es ist deshalb für die Durchsetzung der informationellen Selbstbestimmung von entscheidender Bedeutung, was unter den Begriffen «Personendaten» und «Bearbeiten» verstanden wird.

Art. 3 lit. a DSG definiert Personendaten als «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». BLECHTA ist der Auffassung, dass unter «Angaben» nur Informationen subsumiert werden können, welche irgendwie auf einem materiellen Träger gespeichert und somit *manifestiert* sind,<sup>436</sup> also wenn es sich um Daten im in dieser Dissertation definierten Sinne handelt.<sup>437</sup> Demgegenüber vertritt ROSENTHAL die Meinung, dass der Informationsträger keine Sache im sachenrechtlichen Sinn sein müsse und beispielsweise die Speicherung einer Information im menschlichen *Gedächtnis* genüge, um die Definition von «Angabe» zu erfüllen.<sup>438</sup> Dieser Meinung ist insoweit zu folgen, als auch personenbezogene Informationen ein Gefährdungspotential für die betroffenen Personen darstellen können und es bei deren grundsätzlichem Ausschluss aus dem Geltungsbereich des DSG zu absurden *Ungleichbehandlungen* kommen kann. So würde die Situation, dass eine psychiatrische Anstalt am Telefon (ohne Aufzeichnung) allerlei Informationen über ihre Klienten bekannt geben darf, nicht unter den Anwendungsbereich des DSG fallen, die Bekanntgabe der selben Daten in Schriftform jedoch schon. Da der offen gehaltene Wortlaut von Art. 3 lit. a DSG eine Subsumtion von Informationen unter den Begriff «Personendaten» zulässt, erscheint es unnötig, die Bestimmung zu revidieren, da sie grundrechtskonform ausgelegt werden kann. Der etwas absurd erscheinende Konsequenz, dass somit jeder personenbezogene Gedanke unter die Anwendbarkeit des DSG fällt, es sei denn, die Person «bearbeitet» die Informationen zum persönlichen

---

<sup>436</sup> BLECHTA, BaKomm DSG/BGÖ, N 6 zu Art. 3 DSG.

<sup>437</sup> Zur Definition von Daten siehe Kapitel IV, Ziffer 6.3.

<sup>438</sup> ROSENTHAL, Handkommentar DSG, N 11 zu Art. 3.



Gebrauch und gibt sie nicht an Aussenstehende bekannt, kann durch eine klare Auslegung des Vorgangs «Bearbeiten» entgegengewirkt werden.<sup>439</sup>

#### 4.1.3 Interpretation «Bearbeiten» nach Art. 3 lit. e DSG<sup>440</sup>

Wie im vorangehenden Abschnitt eingangs erläutert, ist es für die Anwendbarkeit des DSG zentral, was unter «Bearbeiten» von Personendaten verstanden wird. Eine klare Auslegung des Begriffs ist auch deshalb von entscheidender Bedeutung, weil die Phänomene «Information» und «Datum» nur schwer voneinander abzugrenzen sind, es aber klare Regeln braucht, wie mit diesen personenbezogenen Angaben umgegangen werden darf, da gerade dieser Umgang persönlichkeitsgefährdend ist.<sup>441</sup>

Bearbeiten wird in Art. 3 lit. e DSG definiert als «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten». Strittig ist, ob auch das bloss *Eindruckerwecken* einer Datenbearbeitung unter diese Begriffsdefinition fällt.<sup>442</sup> Darüber hinaus stellt sich die Frage, ob auch ein reines *Gedankenspiel* oder eine rein akustische Wahrnehmung unter den Begriff «Bearbeiten» zu subsumieren ist und damit unter den Anwendungsbereich des DSG fällt. Eine derart weite Interpretation des Begriffs scheint übertrieben. Auch unter dem DSG sind die Gedanken frei und der rein gedankliche Umgang mit Personendaten stellt kein Datenbearbeiten im Sinne dieses Gesetzes dar. So kann etwa nicht von einem Datenbearbeiten im Sinne des DSG gesprochen werden, wenn jemand personenbezogene Daten oder Informationen, welche er im Rahmen seiner Tätigkeit zur Kenntnis genommen hat, in seiner Erinnerung ablegt, selbst wenn dies ein erhebliches Risiko für eine persönlichkeitsverletzende Verwen-

---

<sup>439</sup> Zur Interpretation von «Bearbeiten» nach Art. 3 lit. e DSG siehe Kapitel VI, Ziffer 4.1.3.

<sup>440</sup> Hierbei geht es zwar nicht um eine Revision des DSG, die Erörterung der Frage, ob eine Anpassung der Auslegung des Begriffs «Bearbeiten» erfolgen soll, findet aufgrund der Zugehörigkeit zur Frage, ob Art. 3 lit. a DSG revidiert werden müsste, aber gleichwohl unter diesem Titel statt.

<sup>441</sup> Zur Schutzbedarfsanalyse siehe Kapitel V.

<sup>442</sup> GERSCHWILER, RZ 3.34.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

beringen kann.<sup>443</sup> Allerdings liegt nach ROSENTHAL sehr wohl ein Bearbeiten im Sinne des DSG vor, wenn ein solcher Gedanke von der denkenden Person personenbezogen zum Ausdruck gebracht wird, also wenn sich der Gedanke beispielsweise in eine Aktennotiz manifestiert. Diese *Manifestation* muss nach ROSENTHAL nicht «sachlicher Natur» sein. Seiner Meinung nach handelt es sich auch um ein Datenbearbeiten, wenn der Gedanke das Verhalten der denkenden Person beeinflusst und sich dieses Verhalten auf eine bestimmte oder bestimmbare Person bezieht, selbst wenn der Gedanke, also die Information selbst, nie nach aussen getreten ist.<sup>444</sup> Als Beispiel sei hier die Entlassung des homosexuellen Hotelgastes genannt, dessen Kündigung nur aufgrund der mündlichen Bekanntgabe seiner Frau an den katholischen Arbeitgeber erfolgt ist.

Wenn man der Auffassung von ROSENTHAL folgen wollte, stellt sich nebst der schwierigen Aufgabe, solche Datenbearbeitungen im Kopf, welche sich nur mittelbar in der Aussenwelt manifestieren, beispielsweise in einem Gerichtsverfahren zu beweisen,<sup>445</sup> auch die Frage, ob nicht noch danach unterschieden werden müsste, ob die denkende Person zu der von ihrem Verhalten betroffenen Person in einem (zumindest potentiellen) Rechtsverhältnis steht oder nicht. So würde es der hier vertretenen Meinung nach den «Bogen überspannen», wenn die Tatsache, dass eine Frau per Zufall im Treppenhaus hört, wie die Nachbarin ihren Mann beschimpft, fremd gegangen zu sein, und die Frau daraufhin den Mann nicht mehr grüsst, als Bearbeiten im Sinne des DSG verstanden würde und dessen Regeln nun darauf angewendet werden müssten.<sup>446</sup> Der hier vertretenen Ansicht nach kann die ausschliesslich gedankliche Informationsverarbeitung aus *Praktikabilitätsgründen*, aber auch aufgrund des *geringeren Gefährdungspotentials* für die Persönlichkeit nicht unter den Anwendungsbereich des DSG fallen und ist somit nicht unter den Begriff «Bearbeiten» zu subsumieren. Wohl vermögen auch rein akustische Informationsverarbeitungen die informationelle Selbstbestimmung und damit die Persönlichkeit zu verletzen, jedoch

---

<sup>443</sup> ROSENTHAL, Handkommentar DSG, N 69 zu Art. 3.

<sup>444</sup> ROSENTHAL, Handkommentar DSG, N 69 zu Art. 3.

<sup>445</sup> ROSENTHAL, Handkommentar DSG, N 69 zu Art. 3.

<sup>446</sup> Es wäre interessant zu erfahren, wie die Frau dem Anspruch auf Löschen nachkommen möchte, wenn sich herausstellt, dass sie falsch gehört hat und sie somit unrichtige Informationen bearbeitet hat.

überschritte es die Möglichkeiten des DSG, welches die allgemeinen Bestimmungen für den Umgang mit Personendaten festlegt, jede Einzelheit regeln zu können. Dies stellt zweifelsfrei eine echte Lücke dar, die der Gesetzgeber nicht vernünftig zu lösen vermag. Es ist deshalb zu überlegen, ob Fälle von Informationsverarbeitungen, die sich nur im Kopf abspielen, sich jedoch in der Realität durch eine entsprechende Handlung manifestieren und dabei die Persönlichkeit der von der Handlung Betroffenen verletzen, in Anwendung der direkten Horizontalwirkung gelöst werden könnten.<sup>447</sup> Allerdings ist darauf hinzuweisen, dass beispielsweise die Kündigung des homosexuellen Hotelgasts nicht per se persönlichkeitsverletzend war.

### **4.2 Kompetenzerweiterung des EDÖB**

Wie unter Kapitel III, Ziffer 2.1 gezeigt, hat der EDÖB nur eine sehr eingeschränkte Kompetenz, sich im Bereich von Datenbearbeitungen durch Private für die Rechte der Betroffenen stark zu machen, u.a. wenn es sich um einen *Systemfehler* handelt.<sup>448</sup> So konstatiert auch der Bundesrat in seinem Bericht über die Evaluation des DSG, dass die Kompetenzen des EDÖB im internationalen Vergleich nicht besonders stark ausgestaltet sind.<sup>449</sup> Um eine echte Stärkung der informationellen Selbstbestimmung herbeiführen zu können, ist es aber von entscheidender Bedeutung, dass sich der einzelne gegen eine drohende Verletzung der informationellen Selbstbestimmung schnell und unbürokratisch zur Wehr setzen kann. Eine Möglichkeit, dies zu gewährleisten, könnte darin bestehen, dem EDÖB die Handlungskompetenz für *jede einzelfallbezogene Rechtsverletzungen* einzuräumen. Dies würde jedoch wohl, auch mit Zusprenkung vermehrter personeller Ressourcen, den gesamten Betrieb des EDÖB lahmlegen. Ein anderer Weg bestünde darin, den Begriff «Systemfehler» weiter auszulegen, so dass auch Verletzungen im Einzelfall darunter subsumiert werden können, wenn die Art der problematischen Datenbearbeitung auch andere Personen betreffen könnte, obwohl es sich nicht um das gleiche System han-

---

<sup>447</sup> Zur direkten Horizontalwirkung siehe Kapitel VI, Ziffer 2.1.

<sup>448</sup> Dies hängt damit zusammen, dass der Gesetzgeber im Rahmen der privaten Datenbearbeitungen ein grosses Gewicht auf die Privatautonomie legte. Erst wenn durch eine private Datenbearbeitung die Persönlichkeit vieler Personen bedroht ist, soll der EDÖB, quasi im öffentlichen Interesse, einschreiten können (Botschaft DSG, S. 479.).

<sup>449</sup> Bericht BR, S. 345.

delt. Nach HUBER zeigt die Entwicklung der Praxis des EDSB bzw. des EDÖB zwischen 1993 und 2013, dass der Begriff «Systemfehler» weit ausgelegt und ein solcher immer dann angenommen werde, wenn durch die Datenbearbeitung in einer Datenbank viele Personen betroffen sind, aber auch wenn durch die fragliche Datenbearbeitung nur wenige Personen direkt betroffen sind, der Sachverhalt sich aber bei vielen anderen Datenbearbeitern in ähnlicher Form ergeben kann.<sup>450</sup> In der Praxis kann sich dieser Einschätzung jedoch nicht halten: Es besteht vielmehr der Eindruck, dass sich Personen häufig an die kantonalen Datenschutzstellen wenden, da sie vom EDÖB kaum Hilfeleistung erfahren.<sup>451</sup> Insoweit wird hier an der Forderung nach einer weiten Auslegung des Begriffs «Systemfehler» festgehalten.

Darüber hinaus müssen dem EDÖB in Bezug auf festgestellte Datenschutzverletzungen durch Private taugliche *Sanktionsmittel* an die Hand gegeben werden, damit die von ihm gemachten Feststellungen auch Beachtung finden. Dabei gehört nebst einem scharfen *Bussenkatalog*<sup>452</sup> sicherlich auch die entsprechende *Verfügungskompetenz* dazu.<sup>453</sup> Ganz in diesem Sinne wurde im März 2014 von Nationalrat Schwaab die parlamentarische Initiative für wirklich abschreckende Sanktionen bei Datenschutzverletzungen eingereicht.<sup>454</sup> Mit zwölf zu neun Stimmen hat es die Staatspolitische Kommission des Nationalrats jedoch vorerst abgelehnt, dem EDÖB die Kompetenz zur Verhängung von Verwaltungsbussen bei Datenschutzverletzungen zu erteilen. Sie möchte es offen lassen, ob die gemachten Forderungen im Rahmen der bevorstehenden Revision des DSG umgesetzt werden, da sich die Frage stelle, ob diese zusätzliche Kompetenz des EDÖB mit seinen übrigen Aufgaben sinnvoll verbinden lasse. Hierzu vertritt die Kommission die Ansicht, dass viele Daten

---

<sup>450</sup> HUBER, BaKomm DSG/BGÖ, N 12 zu Art. 29 DSG.

<sup>451</sup> So wurden Personen offenbar schon auf ein Merkblatt verwiesen, wenn sie sich über die Videokameras auf den Toiletten bei McDonald's beschwerten.

<sup>452</sup> So sah Art. 79 des ursprünglichen Entwurfs der EU-Datenschutzgrundverordnung vor, dass Unternehmen künftig für Datenschutzverletzungen bis zu 2 % ihres weltweiten Jahresumsatzes oder bis einer Millionen Euro Bussgeld bezahlen müssen. Die Version vom 30. Juni 2014 lässt im neuen Art. 79a die Höhe der Bussgelder offen, da sich die Mitgliedstaaten diesbezüglich (noch) nicht einig sind.

<sup>453</sup> Vgl. auch HUBER, BaKomm DSG/BGÖ, N 44a zu Art. 29 DSG, und BRUNNER, RZ 52, die eine Verfügungsmöglichkeit des EDÖB als wünschbar erachten.

<sup>454</sup> Geschäftsnummer 14.404.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

von den Bürgerinnen und Bürgern freiwillig zur Verfügung gestellt würden und vor allem die Selbstverantwortung des mündigen Bürgers gefordert sei.<sup>455</sup> In Anbetracht der Phänomene «big data»<sup>456</sup> und des ausgewiesenen Schutzbedarfs<sup>457</sup> ist diese Haltung vehement abzulehnen, und es ist zu hoffen, dass der Gesetzgeber bei der Revision des DSG mit mehr Weitsicht an die Sache herangeht und die notwendigen Sanktionsinstrumente einführt.

Um die bereits angesprochene Schwierigkeit, dass sich ein Personendatum gleich auf mehrere Personen bezieht, jedoch nicht alle Betroffenen in die fragliche Datenbearbeitung durch Private einwilligen oder/und es sich als unverhältnismässig schwierig erweist, alle Betroffenen um Einwilligung zu ersuchen, zu lösen, müsste dem EDÖB eine diesbezügliche *Entscheidungskompetenz* zugesprochen werden. Im Falle von Einigungsschwierigkeiten mehrerer Betroffener wäre es an ihm, eine *Interessenabwägung* vorzunehmen. Hinsichtlich der Frage, ob das Einholen aller Einwilligungen unverhältnismässig schwierig ist, müsste er eine diesbezügliche Entscheidung fällen und, sofern der Gesetz- oder Ordnungsgeber nicht gleich Anhaltspunkte geliefert hat, was unter «unverhältnismässig schwierig» zu verstehen ist, eine dementsprechende Praxis entwickeln.

### 4.3 Fazit

Bereits ein Paradigmawechsel des DSG hin zu einer opt-in-Lösung, eine weite Auslegung der Begriffe «Personendaten» und «Systemfehler» sowie eine klare Auslegung des Begriffs «Bearbeiten» vermögen die informationelle Selbstbestimmung im Bereich privater Datenbearbeitungen zu stärken. Mit der Einführung zusätzlicher Kompetenzen für den EDÖB und griffigen Sanktionsinstrumenten würde dem Grundrecht jedoch noch mehr Achtung verschafft werden, da eine Datenschutzverletzung nicht mehr als «Kavaliersdelikt» abgetan werden könnte, sondern die Verursacher empfindlich treffen würde.

---

<sup>455</sup> Bericht der Staatspolitischen Kommission vom 31. Oktober 2014 zur parlamentarischen Initiative 14.404.

<sup>456</sup> Zum Phänomen «big data» siehe Kapitel V, Ziffer 7.

<sup>457</sup> Zum Schutzbedarf siehe Kapitel V.

## 5 Wirksame Selbstregulierung

Wie u.a. im Kapitel III, Ziffer 2.1 gezeigt wurde, ist die Position der Betroffenen im Hinblick auf die Geltendmachung und Durchsetzung ihres Rechts auf informationelle Selbstbestimmung – vor allem wenn es um die Datenbearbeitung durch Privatpersonen geht – sehr unbefriedigend. Unbestrittene Voraussetzung für die Stärkung des Rechts auf informationelle Selbstbestimmung durch eine wirksame Selbstregulierung ist deshalb das Schaffen von *Waffengleichheit*, was bedeutet, dass die Position der Betroffenen gegenüber den potentiellen privaten oder staatlichen Rechtsverletzer soweit gestärkt wird, bis die für die Schlacht benötigten Spiesse gleich lang sind.<sup>458</sup> Dies kann zum einen dadurch geschehen, dass den betroffenen Personen wirksame Instrumente an die Hand gegeben werden, um sich gegen eine widerrechtliche Datenbearbeitung zu wehren (siehe sogleich Ziffer 5.1). Gleich lange Spiesse können etwa aber auch dadurch herbeigeführt werden, dass der Anreiz für die Verwendung von Personendaten gedrosselt wird, indem die Betroffenen finanziell entschädigt oder an den Gewinnen beteiligt werden (siehe sogleich Ziffer 5.2).

### 5.1 Herabsenkung prozessualer Risiken

Einer der Gründe, weshalb in der Schweiz nicht übermässig viele Urteile wegen rechtswidrigem Umgang mit Personendaten gefällt werden, also überhaupt erst einem Gericht zur Beurteilung vorgelegt werden, ist in den nicht zu unterschätzenden prozessualen Hürden zu sehen. Dazu gehören u.a. die *hohen Prozesskosten* sowie die *unattraktiven Klagemöglichkeiten*.<sup>459</sup> Hinzu treten können ausserdem Schwierigkeiten beim *Schadenersatz*. Gerade bei Persönlichkeitsverletzungen ist es schwer, einen finanziellen Schaden überhaupt auszumachen, geschweige denn einen solchen zu beweisen. Aber auch Ansprüche aus Genugtuung (Art. 49 OR) sind nicht wirklich zielführend, da durch den Umstand, dass etwas in ein vom Betroffenen ungewolltes Licht gezogen worden ist, diesem keinen körperlichen Schmerz zufügt, was den klassischen Anwendungsbereich dieses Anspruchs darstellt.<sup>460</sup> Hinzu

---

<sup>458</sup> RUDIN, Datenschutzaufsicht, S. 407.

<sup>459</sup> Zum hürdenreichen Rechtsschutz in der Schweiz siehe RUSCH, S. 139.

<sup>460</sup> DRUEY, Strukturelle Schwächen, S. 150 f.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

kommt, dass der zu erlangende Schadenersatz meist auf den erlittenen materiellen oder immateriellen Schaden begrenzt ist,<sup>461</sup> dieser aber eben schwer zu benennen oder zu beziffern ist,<sup>462</sup> womit sich der finanzielle Aufwand für die Geschädigten im Vergleich zum erwartenden Prozessgewinn nicht lohnt.<sup>463</sup> Aber auch bei einem Zusammenschluss der Betroffenen bei sog. *Massen- oder Streuschäden*, welche aufgrund der heute weit verbreiteten Informationsbeschaffungen durch private Grossunternehmen oder den Staat bei rechtswidrigen Datenbearbeitungen die Regel sein dürften, erscheinen die bestehenden Instrumente als ungenügend oder gar untauglich.<sup>464</sup> Dies wiederum führt dazu, dass die Schadensverursacher nicht mit einer Inanspruchnahme durch die Geschädigten rechnen, womit sie kaum Anreize haben, ihr rechtswidriges Verhalten anzupassen.<sup>465</sup> Ja, es kann gar sein, dass das Datenbearbeiten entgegen dem Recht auf informationelle Selbstbestimmung ein Unternehmen günstiger kommt, als ein rechtmässiges Vorgehen. Während sich in den USA in solchen Fällen der Druck auf die Firmen erhöht, da sie mit hohen Schadenersatzklagen rechnen müssen, bleibt der Rechtsschutz in der Schweiz, aber auch im restlichen Europa «auffällig wirkungsarm».<sup>466</sup>

---

<sup>461</sup> RUDIN, Datenschutzaufsicht, S. 408; nach DRUEY könnte im informationellen Bereich die Genugtuung erst dann helfen, wenn ihr neben der tröstenden Funktion auch klar diejenige einer Privatstrafe zuerkannt würde (DRUEY, Strukturelle Schwächen, S. 151).

<sup>462</sup> Im Entscheid 8G.60/2003 hatte das Bundesgericht über die Höhe einer Genugtuung eines Ehepaars zu entscheiden, welches in einem anonymen Brief beschuldigt wurde, Al-Qaïda-Mitglied zu sein. Nebst der Überwachung des Fernmeldeverkehrs und der Auswertung ihrer Informatikmittel wurde die Frau an ihrem Arbeitsplatz verhaftet, der Mann kurze Zeit darauf in der ehelichen Wohnung im Beisein ihrer 9-jährigen Tochter. Die durchgeführten polizeilichen Ermittlungen ergaben jedoch keine stichhaltigen Hinweise darauf, dass die im Schreiben erhobenen Vorwürfe wahr sein könnten. Das Verfahren wurde deshalb eingestellt. Den Eheleuten wurde eine Genugtuungssumme von SFr. 2000.- zugesprochen plus eine Anwaltsentschädigung von SFr. 800.-.

<sup>463</sup> DRUEY macht in diesem Zusammenhang geltend, dass selbst dort, wo ein solcher Schaden entsteht, als Beispiel nennt er Unternehmensgeheimnisse und die Verkäuflichkeit von Fotos und Stories, der Ausgleich nicht das eigentliche Schutzgut trifft und aufgrund der Natur der «Sache» eine naturale Wiederherstellung ausgeschlossen ist (DRUEY, Strukturelle Schwächen, S. 150 f.).

<sup>464</sup> Bericht BR, S. 2.

<sup>465</sup> Vgl. Bericht BR, S. 13.

<sup>466</sup> RUDIN, Datenschutzaufsicht, S. 409 mit der Erwähnung, dass es Bände spreche, wenn ein Geschäftsleitungsmitglied eines international tätigen Grossunternehmens im persönlichen Gespräch bekenne, sein Unternehmen habe sich nach jenen «regulations» zu richten, bei deren Nichtbeachtung für das Unternehmen die grösste Gefahr drohe, und das seien im Bereich der

### 5.1.1 Stärkung des kollektiven Rechtsschutzes

#### 5.1.1.1 Klagemöglichkeiten

Im Gegensatz zu zahlreichen ausländischen Rechtsnormen sind dem schweizerischen Recht allgemeine repräsentative *Gruppenklagen* nicht bekannt, obwohl sie gemäss dem Bericht des Bundesrates mit dem geltenden Recht durchaus kompatibel wären.<sup>467</sup> In diesem Zusammenhang wäre eine Art Sammelklage besonders bei Unterlassungs-, Beseitigungs- und Feststellungsklagen, ggf. auch bei Genugtuungsklagen ein taugliches Mittel, um effektiv und mit angemessenem finanziellem Aufwand Ansprüche durchzusetzen.<sup>468</sup> Sollen solche Ansprüche auf dem Zivilprozessweg Durchsetzung finden, sieht die ZPO zwar die Verbandsklage (Art. 89 ZPO) sowie die Streitgenossenschaft (Art. 70 ff. ZPO) als Instrumente für die Geltendmachung von Ansprüchen mehrerer Betroffener in einen einzigen Verfahren vor, diese erlangen jedoch aufgrund der ihnen anhängenden Defizite nicht die gewünschte Bedeutung.<sup>469</sup>

Nach Art. 89 Abs. 1 und 2 ZPO können Vereine und andere Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die nach ihren Statuten zur Wahrung der Interessen bestimmter Personengruppen befugt sind, in eigenem Namen auf Unterlassung, Beseitigung und Feststellung der Widerrechtlichkeit von Persönlichkeitsverletzungen klagen. Dabei soll das Erfordernis der gesamtschweizerischen oder regionalen Bedeutung verhindern, dass ad hoc-Verbände zur Klageeinreichung gebildet werden,<sup>470</sup> was jedoch bei der Entdeckung von rechtswidrigen Datenbearbeitungen möglich sein müsste. Im Gegensatz zu Sammelklagen nach amerikanischem Recht zeitigen die mittels der *Verbandsklage* erwirkten Entscheide jedoch

---

Datenbearbeitung klar weder die schweizerischen Rechtsbestimmungen noch die der Europäischen Union; zur Rentabilität von Privatsphärenverletzungen siehe auch DIGGELMANN, S. 76 ff.

<sup>467</sup> Bericht BR, S. 2; dies gilt jedoch nicht für das Vorbild des kollektiven Rechtsschutzes das US-amerikanische Instrument der class action. Diese wird für die Schweiz als weder nötig noch erstrebenswert angesehen und gar im Ganzen abgelehnt (Bericht BR, S. 40); ferner ist darauf hinzuweisen, dass der Vorentwurf zum DSG noch eine ausdrückliche Regelung des Klagerrechts für Verbände beinhaltet hat (Botschaft DSG, S. 465).

<sup>468</sup> WIDMER, S. 83.

<sup>469</sup> Bericht BR, S. 2.

<sup>470</sup> SPÜHLER, BaKomm ZPO, N 11 zu Art. 89 ZPO.



## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

auch nur unter den Prozessbeteiligten Wirkung.<sup>471</sup> Wird also beispielsweise festgestellt, dass eine Krankenkasse ihre Kundendaten an ein Pharmaunternehmen verkauft, so profitieren vom rechtlichen Entscheid nur die klagenden Personen und nicht auch gleich alle anderen von der rechtswidrigen Datenbearbeitung Betroffenen. Darüber hinaus ist zu bemerken, dass mit dieser Klagemöglichkeit Geldleistungen, sei es in Form von Schadenersatz, Genugtuungsleistungen oder Gewinnherausgabe, nicht geltend gemacht werden können,<sup>472</sup> weshalb sie für die Klagenden, welche Geld in die Hand nehmen müssen, um überhaupt die Widerrechtlichkeit zu beanstanden, nicht interessant ist.

Bei der *Streitgenossenschaft* nach Art. 70 ff. ZPO ist zwischen notwendiger und einfacher Streitgenossenschaft zu unterscheiden. Während bei der notwendigen Streitgenossenschaft zwingend mehrere Personen gemeinsam als Kläger auftreten müssen, was voraussetzt, dass das eingeklagte Recht nur von mehreren Personen gemeinsam oder nur gegen mehrere Personen gemeinsam ausgeübt werden kann, können bei der einfachen Streitgenossenschaft mehrere rechtlich voneinander unabhängige, aber sachlich zusammenhängende Klagen in einem Prozess zusammengefasst werden. Diese letztgenannte Form der Streitgenossenschaft entsteht somit entweder aufgrund gemeinsamer Klageerhebung durch die beteiligten Parteien oder aufgrund der Vereinigung getrennt eingereichter Klagen durch das zuständige Gericht.<sup>473</sup> Das Vorgehen im Rahmen einer Streitgenossenschaft setzt somit voraus, dass sich die Betroffenen finden und organisieren, was jedoch in der Realität oft aufwändig und mit einigen Schwierigkeiten verbunden ist, denn auch wenn der einzelne weiss, dass noch andere von der unrechtmässigen Datenbearbeitung betroffen sind, kennt er weder deren Namen noch Adressen, um sich mit ihnen in Verbindung zu setzen, von der Arbeit diese zu kontaktieren und sie zum Mitstreiten zu überzeugen ganz abgesehen.<sup>474</sup>

Der Bundesrat hat immerhin in seinem Bericht anerkannt, dass diese Klagemöglichkeiten aufgrund der heutigen Gefährdungen nur mässig adäquat und dass Anpas-

---

<sup>471</sup> SPÜHLER, BaKomm ZPO, N 2 zu Art. 89 ZPO.

<sup>472</sup> Bericht BR, S. 26.

<sup>473</sup> WIDMER, S. 85.

<sup>474</sup> M.w.H. Bericht BR, S. 20.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

sungen unumgänglich sind. Deshalb erwägt er mit Blick auf die Verbandsklage eine Erweiterung des sachlichen und inhaltlichen Anwendungsbereichs. Ausserdem schlägt er die Prüfung von neuen Instrumenten für eine echte kollektive Rechtsdurchsetzung vor, wobei er in diesem Zusammenhang Opt-in-Gruppenklagen oder Gruppenvergleichsverfahren nennt.

Rechtswidrige Datenbearbeitungen, welche häufig eine Vielzahl von Personen betreffen, sind nicht nur im Privatrechtsbereich anzutreffen. Auch der Staat ist davor nicht gefeit, zumal er immer mehr Tätigkeiten im Rahmen des new public management an Private auslagert und de facto häufig die effektive Kontrolle über deren Handlungen verloren haben dürfte. Deshalb muss hier auch gefragt werden, inwieweit nicht auch im Verwaltungsprozess kollektive Rechtsmittel wirkungsvolle Instrumente in Bezug auf die Verbesserung des Schutzes der erweiterten Persönlichkeit und damit der Durchsetzung der informationellen Selbstbestimmung sein könnten.<sup>475</sup>

### 5.1.1.2 Prozesskosten

Nach Art. 98 ZPO kann das Gericht von der klagenden Partei einen *Vorschuss* bis zur Höhe der mutmasslichen *Gerichtskosten* verlangen, wovon heute in vielen Fällen Gebrauch gemacht wird.<sup>476</sup> Bereits dieser Vorschuss kann die klagende Partei in finanzielle Schwierigkeiten bringen. Im Hinblick darauf, dass dieser im Falle eines Unterliegens gänzlich von ihr zu tragen wäre und sie darüber hinaus auch noch eine *Parteientschädigung* an die Gegenpartei entrichten müsste (Art. 106 Abs. 1 ZPO), dürfte das finanzielle Risiko vielen Betroffenen zu hoch sein. Dies gerade auch deshalb, weil eine Verletzung der Persönlichkeit durch unrechtmässiges Datenbearbeiten im Gegensatz zu einem Blechschaden am Auto schwer zu beweisen und der Schaden kaum zu beziffern ist.<sup>477</sup>

Im Rahmen der Streitgenossenschaft sieht Art. 93 Abs. 1 ZPO zwar für die Ermittlung des Streitwertes vor, dass die geltend gemachten Ansprüche zusammengezählt werden und die Beteiligten somit angesichts der degressiven Tarife für die Prozess-

---

<sup>475</sup> Vgl. WIDMER, S. 85; Bericht BR, S. 56.

<sup>476</sup> M.w.H. Bericht BR, S. 43.

<sup>477</sup> Vgl. Motion von Jean Christophe Schwaab vom 7. März 2013, Recht zur Sammelklage bei Datenschutzverletzungen, insbesondere im Internet, Geschäftsnummer 13.3052.

kosten im Vergleich zur individuellen Klageerhebung profitieren. Es ist jedoch zu berücksichtigen, dass diesen Kostenvorteilen finanzielle Auslagen für die Prozessorganisation und -administration gegenüberstehen. Ausserdem führt die Möglichkeit der solidarischen Haftung der Streitgenossen nach Art. 106 Abs. 3 ZPO dazu, dass für den einzelnen ein deutlich höheres *Prozesskostenrisiko* entsteht.<sup>478</sup>

Auch in Bezug auf die Prozesskosten hat der Bundesrat Handlungsbedarf erkannt. So zieht er in Betracht, die Gerichtskostenvorschusspflicht nach Art. 98 ZPO so anzupassen, dass eine Vorschusspflicht bei Klageerhebung durch eine Streitgenossenschaft bei Massenschäden nur noch ausnahmsweise bestünde. Ebenfalls ist angedacht, die Solidarhaftung nach Art. 106 Abs. 3 ZPO bei kollektiver Klageerhebung im Rahmen der Streitgenossenschaft abzuschaffen.<sup>479</sup>

### 5.1.1.3 Beweisschwierigkeiten

Wie bereits erwähnt ist die Beweisführung bei Klagen auf Verletzung der Persönlichkeit wegen unrechtmässiger Datenbearbeitung im Rahmen von Art. 28 ZGB schwierig. Dies hängt damit zusammen, dass der Betroffene sowohl die unzulässige Datenbearbeitung wie auch die diesbezügliche Mitwirkung des Beklagten darlegen muss. Die befürchtete Persönlichkeitsverletzung muss dabei vom Kläger genau umschrieben werden. Bei den von den Klägern zu beweisenden schädigenden Handlungen handelt es sich jedoch nicht selten um Abläufe, welche sich im Innern des Herrschaftsbereichs des Beklagten abspielen, deren Beweis vielfach spezielles technisches Knowhow voraussetzen. «Es ist einfacher zu beweisen, dass ein Baukran einen Betonmischer auf das Nachbarhaus hat fallen lassen»,<sup>480</sup> als dass eine Zusatzversicherung Daten aus dem Pool der obligatorischen Krankenversicherung für die Überprüfung ihrer Rechnungspflicht verwendet hat, obwohl sie dazu keine Einwilligung hatte. Auch kann in Anbetracht der vorhandenen technischen Möglichkeiten die Rückverfolgbarkeit auf den potentiellen Täter weitgehend ausgeschlossen werden.<sup>481</sup> Um hier einen effizienteren Schutz zu gewährleisten, müsste Art. 28 ZGB um eine

---

<sup>478</sup> M.w.H. Bericht BR, S. 21.

<sup>479</sup> Bericht BR, S. 45 f.

<sup>480</sup> RUDIN, Datenschutzaufsicht, S. 409.

<sup>481</sup> Vgl. Botschaft DSG, S. 417.

*Beweislasterleichterung* sowie eine *Beweislastumkehr* erweitert werden, so dass die Kläger bei einem Beseitigungsanspruch die persönlichkeitsverletzende Datenbearbeitung «nur» glaubhaft machen müssen und es Sache des Beklagten ist, die Rechtfertigung für die Datenbearbeitung zu beweisen. Bei einem Unterlassungsanspruch könnten die Kläger die Datenbearbeitung verbieten und der Beklagte müsste darlegen, weshalb er das Recht zur Datenbearbeitung hat.<sup>482</sup>

### 5.1.2 Herabsetzung der prozessualen Risiken für die Einzelperson

Aber nicht nur im Bereich der kollektiven Klagemöglichkeiten ist Handlungsbedarf vorhanden. Auch und soweit es um Persönlichkeitsverletzungen durch Einzelpersonen geht, welche nicht auf einem Systemfehler beruhen, bestehen für die Betroffenen hohe Hürden, welche vor allem in den hohen Prozesskosten sowie den Beweisschwierigkeiten zu sehen sind. Gerade als Einzelperson ist das *finanzielle Risiko*, das mit der Führung eines Prozesses einhergeht, abschreckend hoch. Dies betrifft nicht nur die Anwalts- und die eigentlichen Gerichtskosten. Auch die *Beweisführung* kann eine beträchtliche Summe in Anspruch nehmen, die dem Gericht vorschussweise zu bezahlen ist (Art. 102 Abs. 1 ZPO). Die unter dem vorangehenden Kapitel gemachten Ausführungen gelten insoweit auch für die Prozessrisiken einer Einzelperson, allerdings hat diese keine Möglichkeit, sich die Kosten und somit auch das Risiko mit anderen Mitstreitern zu teilen. Art. 107 Abs. 1 lit. b ZPO sieht zwar die Möglichkeit vor, dass das Gericht die Prozesskosten verteilen kann, wenn eine Partei in guten Treuen zur Prozessführung veranlasst war. Ebenfalls sieht die ZPO die Möglichkeit der *unentgeltlichen Rechtspflege* vor, wenn einer Person die erforderlichen Mittel fehlen und ihr Begehren nicht aussichtslos erscheint (Art. 117 ZPO). Die betroffenen Personen sind jedoch vielfach nicht in einer derart schlechten finanziellen Lage, dass diese Bestimmung zur Anwendung käme. Vielmehr ist es so, dass die mit einer Klage verursachten Kosten dem einzelnen im Vergleich zum möglichen ma-

---

<sup>482</sup> POLEDNA/CODONI, S. 272; dieses Vorgehen wäre wiederum konsistent mit der vorgeschlagenen Anpassung von Art. 12 DSG (Kapitel VI, Ziffer 4.1.1); vgl. die Möglichkeit nach Art. 261 Abs. 1 ZPO, wonach das Gericht die notwendigen vorsorglichen Massnahmen trifft, wenn die gesuchstellende Partei *glaubhaft* macht, dass ein ihr zustehender Anspruch verletzt ist oder eine Verletzung zu befürchten ist und ihr aus der Verletzung ein nicht leicht wieder gutzumachender Nachteil droht.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

teriellen wie auch immateriellen Gewinn zu hoch sind, auch wenn er sich die Prozessführung leisten könnte, und er deshalb auf die Ausübung seines Rechts verzichtet. Man kann nun darüber diskutieren, ob der Staat in irgendeiner Weise tätig werden muss, wenn die Verteidigung seines Rechts schon nicht mal dem Betroffenen selbst viel wert ist. Bei dieser Diskussion gilt es allerdings zwei Dinge zu beachten: Als erstes handelt es sich bei solchen Prozesskosten nicht um Lappalien. Auch wenn man davon ausgehen könnte, dass solche Beträge von einem Durchschnittsverdiener durchaus aufgewendet werden könnten,<sup>483</sup> so stellen Prozesskosten zumindest hierzulande nur selten eines jener Risiken dar, für die man grundsätzlich Geld auf die Seite legt. Darüber hinaus hat die Wahrung der informationellen Selbstbestimmung wie im Rahmen der Schutzbedarfsanalyse dargestellt,<sup>484</sup> auch eine gesellschaftliche Funktion, weshalb es legitim erscheint, die mit der Geltendmachung dieses Rechts entstehenden Kosten nicht alleine den Betroffenen aufzubürden, sofern sie ihr Recht in guten Treuen wahrnehmen wollen.

In Anbetracht dieser Ausführungen wird deshalb vorgeschlagen, das Zivilprozessrecht dahingehend zu ergänzen, dass das *vereinfachte Verfahren* nach Art. 243 ff. ZPO bei Persönlichkeitsverletzungen durch den widerrechtlichen Umgang mit Daten oder Informationen generell zum Tragen kommt und nicht nur bei Streitigkeiten zur Durchsetzung des Auskunftsrechts nach dem DSG (Art. 243 Abs. 2 ZPO). Durch die besonderen Kennzeichen diese Verfahrensart, wie die erleichterte Form (Art. 244 ZPO), die vorherrschende Mündlichkeit (Art. 245 ZPO) und die verstärkte Prozessleitung (Art. 247 ZPO), besteht ein schneller und unbürokratischer Weg ans Gericht, womit auch eine Senkung der Prozesskosten möglich sein sollte (weil beispielsweise auf den Beizug eines Anwalts verzichtet werden kann). Darüber hinaus sollte eine drohende Persönlichkeitsverletzung der beschriebenen Art im Rahmen des *summarischen Verfahrens* nach Art. 248 ff. ZPO geltend gemacht werden können, da sie so ggf. noch abwendet werden kann.

---

<sup>483</sup> Bereits diese Annahme muss jedoch in Frage gestellt werden, lebt doch ein Grossteil der sog. Mittelschicht nur gerade von der Hand in den Mund, und vermag es nicht, Vermögen anzusparen (S. 12 des Schlussberichts zur Studie «Wie geht es den Mittelschichtfamilien in der Schweiz» des GfS Bern).

<sup>484</sup> Siehe Kapitel V.

### 5.1.3 Fazit

Die bestehenden prozessualen Möglichkeiten bei Persönlichkeitsverletzungen durch den Umgang mit Daten und Informationen sind ungenügend, die Prozessrisiken hoch und die Beweiserbringung schwer, weshalb die Betroffenen nur selten den Gerichtsweg beschreiten. Dies wiederum führt dazu, dass auf Verletzerseite das Risiko, sich in einem Prozess verantworten zu müssen, als so gering eingestuft wird, dass kaum Anreiz geschaffen wird, den fraglichen Umgang mit Personendaten oder Personeninformationen verfassungskonform auszugestalten. Um dieses Manko zu beseitigen, braucht es vereinfachte Verfahren, die eine rasche und unkomplizierte gerichtliche Beurteilung zulassen, damit zusammenhängend eine Senkung der Prozesskosten sowie Beweiserleichterungen. Immerhin im Bereich des kollektiven Rechtsschutzes hat der Bundesrat den Handlungsbedarf erkannt, auch wenn derzeit noch unklar ist, wie genau und bis wann er den Defiziten beikommen möchte.

## 5.2 *Herausgabe vermögenswerter Vorteile*

Das Inaussichtstellen vermögenswerter Vorteile oder Einbussen ist ein erprobtes Mittel, um das menschliche Verhalten zum rechtlich Erwünschten beeinflussen zu können.<sup>485</sup> Es ist deshalb nachfolgend zu prüfen, ob dieses Instrument auch zur Stärkung der informationellen Selbstbestimmung tauglich wäre. In diesem Sinne THALER: «Nicht zu leugnen ist die wachsende Kommerzialisierung des Höchstpersönlichen, die soziale Geltung als Vermögenswert. (...) Der Kreis der Persönlichkeitselemente, die Gegenstand der Kommerzialisierung bilden, sind nicht auf Bildnis, Namen und Stimme beschränkt.»<sup>486</sup>

### 5.2.1 Right of Publicity in den USA

In den USA können vermögenswerte Rechte der Persönlichkeit mit dem je nach Bundesstaat unterschiedlich ausgestalteten Right of Publicity geltend gemacht werden. 1953 erkannte ein amerikanisches Gericht im Entscheid *Haelan Laboratories*,

---

<sup>485</sup> Zu denken sind an die diversen Bussgelder im Straf- und Nebenstrafrecht sowie in umgekehrter Form die Subventionen.

<sup>486</sup> THALER, S. 87.

Inc. versus Topps Chewing Gum, Inc. ein vom Right of Privacy getrenntes «geldwertes Ausschliesslichkeitsrecht an der eigenen Identität».<sup>487</sup> In der Sache ging es um zwei rivalisierende Kaugummiproduzenten, welche versucht hatten, die Rechte für die Verwendung von Bildern verschiedenster Baseballspieler für ihre jeweiligen Sammelkarten zu erlangen. Haelan Laboratories, Inc. hatte dabei die Exklusivrechte von verschiedenen Spielern erworben, wogegen Topps Chewing Gum, Inc. argumentierte, dass es dem Kläger an einem exklusiven property right fehle und es ihm zustehe, ebenfalls Verträge mit den selben Spielern abzuschliessen. Das Gericht stützte die Klage von Haelan Laboratories, Inc. folgendermassen: «We think that in addition to and independent of that right of privacy (...), a man has a right in the publicity value of his photograph (...).»<sup>488</sup> 1995 hat das American Law Institute das Right of Publicity als *intellectual property law* anerkannt und in das Restatement of Unfair Competition aufgenommen.<sup>489</sup> Mit der Berufung auf das Right of Publicity kann eine Person nun ein Ausschliesslichkeitsrecht (aber kein Eigentumsrecht) geltend machen,<sup>490</sup> welches die das Datum (Bild, Name, Pseudonym, Stimme etc.) verwendende Person dazu verpflichtet, die vermögenswerten Vorteile, welche durch die Datumsverwendung erlangt worden sind, herauszugeben. Dabei muss er allerdings nachweisen, dass ihm durch die Verwendung seines Datums *finanzielle Einbussen* entstanden sind oder entstehen können.<sup>491</sup> Letztere Voraussetzung führt dazu, dass sich vor allem Prominente auf diese Klage stützen können, bei allen andern wird die Verwendung der eigenen Daten, ausser im Kontext mit Werbung, kaum zu vermögensrechtlichen Einbussen führen.

---

<sup>487</sup> MEYER, RZ 174 mit Verweis auf United States Court of Appeals Second Circuit, Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866.

<sup>488</sup> MEYER, RZ 174 mit Verweis auf United States Court of Appeals Second Circuit, Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, S. 868.

<sup>489</sup> MEYER, RZ 200 mit weiteren Verweisen.

<sup>490</sup> MEYER, RZ 298.

<sup>491</sup> MEYER, RZ 350 ff.

### 5.2.2 Vermögenswerte Persönlichkeitsrechte in Deutschland

Spätestens mit dem Marlene Dietrich-Urteil von 1999 anerkennt auch der Bundesgerichtshof vermögenswerte Bestandteile des Persönlichkeitsrechts.<sup>492</sup> Dabei ging es um die Verwendung des Bildes, Namens und Namenszuges von Marlene Dietrich nach ihrem Tod durch die Lighthouse Musical Produktionsgesellschaft mbH im Rahmen eines Musicals und zu Werbezwecken. Der Bundesgerichtshof machte dabei deutlich, dass das Persönlichkeitsrecht zwar in erster Linie ideellen Interessen diene, darüber hinaus könne aber Name, Abbildung und weiteren Merkmalen der Persönlichkeit ein beträchtlicher *wirtschaftlicher Wert* zukommen, den es auch abzugelten gelte.<sup>493</sup> BEUTHIEN macht sodann einen Unterschied zwischen der Persönlichkeit als Teil der Person, welche neben Leben, Körper und Gesundheit ein personales Schutzgut darstelle, das höchstpersönlich sei und sich nicht vermögensrechtlich schützen lasse, und dem *Persönlichkeitsbild*, dem Image, das bei den Mitmenschen entstehe, welches sich als unkörperlicher Gegenstand mit wirtschaftlichem Zuweisungsgehalt begreifen lasse, bezüglich dem der Person ein *eigentumsähnliches Persönlichkeitsgüterrecht* zustehe.<sup>494</sup> Jedoch stellt nicht jedes persönliche Datum bereits ein Persönlichkeitsgut dar, vielmehr müssen es besondere eigenpersönliche Daten von wirtschaftlichem Wert sein.<sup>495</sup> Eine positivrechtliche Regelung, welche ausdrücklich vermögenswerte Bestandteile des Persönlichkeitsrechts anerkennt, fehlt in Deutschland aber immer noch.<sup>496</sup>

### 5.2.3 Vermögenswerte Persönlichkeitsrechte in der Schweiz

In der Schweiz hat im Unterscheid zu den USA und Deutschland schon der Gesetzgeber auf die möglichen vermögensrechtlichen Konsequenzen in Folge einer Persönlichkeitsverletzung Bezug genommen.<sup>497</sup> *Art. 28a Abs. 3 ZGB* sei in diesem Sinne als Einsicht des Gesetzgebers zu lesen, dass der Zugriff auf personale Güter die Form

---

<sup>492</sup> Urteil des BGH vom 1. Dezember 1999, Aktenzeichen: 1 ZR 149/97.

<sup>493</sup> Urteil des BGH vom 1. Dezember 1999, Aktenzeichen: 1 ZR 149/97, E. II 1.

<sup>494</sup> BEUTHIEN, NJW 2003, S. 1221 ff.

<sup>495</sup> BEUTHIEN/SCHMÖLZ, 50.

<sup>496</sup> MEYER, RZ 522.

<sup>497</sup> MEYER, RZ 708.



## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

der wirtschaftlichen Ausbeutung verwertbarer Positionen annehmen kann.<sup>498</sup> Eine nicht gerechtfertigte kommerzielle Nutzung individualisierender Persönlichkeitsaspekte stellt demnach einen Eingriff in das persönliche Selbstbestimmungsrecht dar und ist per se als Persönlichkeitsverletzung anzusehen.<sup>499</sup> Denn gerade weil Personendaten wie Name, Bild etc. eine Person kennzeichnen und auf sie zurückweisen, müssen die aus diesen Daten gewonnenen Werte auch diesen Personen zugeordnet werden.<sup>500</sup> Während ältere Bundesgerichtsentscheide die Rechtswidrigkeit der *Fremdkommerzialisierung* von Name und Bild noch mit der *Ansehensminderung* der verletzen Person begründen, erwägen jüngere Urteile ein Recht auf *Selbstpräsentation* und die *Allokationsgerechtigkeit*.<sup>501</sup> In BGE 133 III 153 ff. anerkannte das Bundesgericht, dass im Bereich des Persönlichkeitsschutzes eine Usurpation im Zusammenhang mit der Verwertung vermögenswerter Nutzungsrechte aus dem Persönlichkeitsrecht möglich sei.<sup>502</sup>

Nach THALER geht es hier um «die ausschliesslichkeitsrechtliche Absicherung des Vermarktungspotentials an der eigenen Persönlichkeit». Seiner Meinung nach sind Parallelen zwischen Persönlichkeits- und Eigentumsschutz klar erkennbar, indem der innere Bereich der Persönlichkeit infolge der steigenden Bedeutung deren Vermarktung immer mehr dem Eigentum – als Eigentum an der eigenen Persönlichkeit – ähnelt. Deshalb sei es auch gerechtfertigt, dass das Persönlichkeitsrecht in seiner ökonomischen Ausprägung dem Eigentum als erarbeitetes Rechtsgut entspricht, so etwa die Popularität eines Spitzensportlers als Ergebnis einer meist langjährigen sportlichen Laufbahn. Denn beide Rechtsinstitute ermöglichen aufgrund ihrer Kapitalisierbarkeit die Teilnahmechance am Wirtschaftsverkehr und somit der *wirtschaftlichen Selbstverwirklichung*. Jede fortdauernde Ungleichbehandlung habe somit rechtstheoretische Legitimationsdefizite zur Folge.<sup>503</sup> Auch MEYER ist der Ansicht, dass das Selbstbestimmungsrecht des einzelnen auch in Bezug auf die von aussen zugeschriebenen Vermögenswerte an seinen Persönlichkeitsrechten Geltung haben

---

<sup>498</sup> BÜCHLER, S. 317.

<sup>499</sup> MEYER, RZ 708 mit Verweis auf BÜCHLER, S. 315.

<sup>500</sup> MEYER, RZ 729.

<sup>501</sup> MEYER, RZ 708 mit Verweis auf BÜCHLER, S. 315.

<sup>502</sup> BGE 133 III 153 ff. (158), E. 2.4.

<sup>503</sup> THALER, S. 88.

muss.<sup>504</sup> BIENE befürwortet dagegen das US-amerikanische Modell mit dem Right of Privacy als Idealschutz und dem Right of Publicity als Vermögensschutz und ist gar der Ansicht, dass sich dieses zweigeteilte Modell ohne strukturelle Widersprüche in die kontinentaleuropäische, als Antipole konstruierte Dogmatik der Herrschafts- und Abwehrrechte einfügen lasse.<sup>505</sup>

### 5.2.4 Fazit

Die Abschöpfung vermögenswerter Vorteile, welche Dritte durch die unerlaubte Verwendung der eigenen Daten erlangt haben, ist in den USA ein gängiges Mittel, um den Anreiz zu mildern, mit etwas Fremden Geld zu verdienen, ohne den eigentlichen «Besitzer» daran teilhaben zu lassen. Dieses Right of Publicity hat allerdings den Nachteil, dass eine finanzielle Einbusse nachgewiesen werden muss, womit dem «Durchschnittsmenschen» diese Klageart verwehrt ist. Obwohl auch der Bundesgerichtshof vermögenswerte Bestandteile des Persönlichkeitsrechts anerkannt hat, fehlt es in Deutschland bis heute an einem formell-gesetzlich normierten Anspruch. Dies im Gegensatz zur Schweiz, wo der Gesetzgeber dem einzelnen in Art. 28a Abs. 3 ZGB einen Anspruch auf Herausgabe des Gewinns aus einer Persönlichkeitsverletzung zusichert. Es ist allerdings zu beachten, dass diese Abschöpfungsmöglichkeiten immer nur bezüglich des erzielten Gewinns aus der Verwendung «spezifischer» Personendaten wie dem Bild, Namen etc. angewendet werden können. Interessant wäre es jedoch, wenn ein Anspruch auf Gewinnabschöpfung auch im Rahmen der Verwendung «unspezifischer» persönlicher Daten, wie sie beim Phänomen «big data» anfallen, bejaht werden würde.

### 5.3 Fazit

Um dem Grundrecht auf informationelle Selbstbestimmung zu verbesserter Durchsetzung zu verhelfen, ist es unabdingbar, dass der einzelne wirksame Instrumente an die Hand bekommt, so dass er sich im Sinne einer Selbstregulierung selbstständig gegen Verletzungen zur Wehr setzen zu kann. Als solche Instrumente kommen

---

<sup>504</sup> MEYER, RZ 729.

<sup>505</sup> BIENE, S. 159 f.

insbesondere ein niederschwelliger Zugang zum Gericht und eine Abschöpfung vermögenswerter Vorteile aus Fremdkommerzialisierung in Betracht. Beide Mittel weisen zwar derzeit noch ihre Schwächen auf, doch können diese mit einem diesbezüglichen gesetzgeberischen Willen ausgemerzt werden.

## 6 Résumé und Überleitung

Die dargestellten Möglichkeiten haben gezeigt, dass diverse Ansätze vorhanden sind, wie die Einflussmöglichkeiten des einzelnen in Bezug auf den Umgang mit den ihn betreffenden Daten und Informationen gestärkt werden können und damit dem Grundrecht auf informationelle Selbstbestimmung zu vermehrter Durchsetzung und Praxistauglichkeit verholfen werden kann. Dies wiederum zeugt davon, dass durchaus der Wille vorhanden ist, an diesem Grundrecht festzuhalten, es gegebenenfalls gar auf eine neue Stufe zu bringen, in dem Sinn, dass dessen elementare Bedeutung für unser aller Zusammenleben wieder in unser alltägliches Bewusstsein rückt. Dazu reicht es der hier vertretenen Auffassung nach jedoch nicht aus, nur eine der gezeigten Ideen umzusetzen. Vielmehr müsste sich der Gesetzgeber ganz klar hinter das Grundrecht stellen und seiner Pflicht, dafür Sorge zu tragen, dass die Grundrechte auch zwischen Privaten wirksam werden, nachkommen. Nebst der Einräumung einer Entscheidungsbefugnis des einzelnen in Bezug auf seine Daten und Informationen im DSG bedürfte es der gezeigten Anpassungen im Prozessrecht sowie einer wie auch immer gearteten Abschöpfungsmöglichkeit des mit den eigenen Daten und Informationen erzielten Gewinns durch Dritte. Diese gezeigten Ansätze sind bewusst vermehrt auf Datenbearbeitungen durch Privatpersonen gerichtet, da in diesem Bereich, der hier vertretenen Auffassung nach, die grösseren Defizite bestehen. Im Rahmen der Abwicklung von staatlichen Aufgaben ändert sich hingegen mit einer Stärkung der informationellen Selbstbestimmung nichts Grundlegendes. Wie gezeigt, können Grundrechte wie dieses nach den Voraussetzungen von Art. 36 BV eingeschränkt werden. Es liegt am Gesetzgeber, die zur Abwicklung der staatlichen Aufgaben notwendigen Einschränkungen zu legiferieren.<sup>506</sup>

---

<sup>506</sup> Zur Art wie er dies zu tun hat siehe Kapitel IV, Ziffer 3.

## VI Vorschläge zur Stärkung des Rechts auf informationelle Selbstbestimmung

Gerade im Gesundheitsbereich finden die Datenflüsse mehrheitlich auf der Basis von Rechtsgrundlagen statt, der Einwilligung kommt hier nur eine sehr untergeordnete Rolle zu. In diesem Bereich wurde eine enge Regulationsdichte offenbar als erforderlich erachtet. Hingegen müssen wir uns vergegenwärtigen, dass durch derartig viele, wenn auch gesetzlich verankerte Datenflüsse der gläserne Bürger, hier der gläserne Patient, nicht mehr weit ist. Die elektronische medizinische Infrastruktur, angefangen von einem ePatientendossier über von Krankenkassen betriebene Apps, welche ihre Kunden an ein gesundheitsbewusstes Verhalten mahnen, bis hin zu den täglich in Betrieb stehenden Praxissystemen, welche gerne an verschiedene weitere Systeme zur Administration der Patientendaten angebunden sind, und die damit einhergehende umfassende Kontrolle unseres Gesundheitszustandes scheint bald umfassend etabliert. Obwohl das Arztgeheimnis als Ausdruck des Vertrauensverhältnisses in der Arzt-Patienten-Beziehung schon seit jeher besonderen Schutz erfahren hat, erweitert sich der Personenkreis, der Zugang zu den Gesundheitsdaten hat, immer mehr. Nicht nur die ärztlichen Hilfspersonen wie Pflegepersonal oder Labormitarbeitende gehören dazu, sondern auch externe Abrechnungsstellen, Kranken- und Unfallversicherungen, aber auch weitere staatliche und nicht-staatliche Stellen.<sup>507</sup> Hinzu kommt, dass all diese Stellen an EDV-Systeme angebunden sind, diese gewartet und betrieben werden müssen und so letztlich eine riesige Zahl von Personen Zugang zu einer riesigen Menge sensibler Gesundheitsdaten hat.

Die folgende Praxisstudie wird anhand eines fiktiven Ausgangsfalls die damit einhergehenden verschiedenen Datenflüsse herausarbeiten, um einerseits aufzuzeigen, wie viel in diesem Bereich der Einflussmöglichkeit des einzelnen verwehrt bleibt, auch wenn das Recht auf informationelle Selbstbestimmung konsequent umgesetzt würde, und andererseits um zu veranschaulichen, wie viele Personen in die Abwicklung dieser Datenflüsse involviert sind und wie viele Daten eigentlich erhoben werden.

---

<sup>507</sup> SCHAAR, S. 73 ff.

## VII Praxisstudie

Ausgangsfall: Eine Frau, alleinstehend, wohnhaft in Basel, sucht die Notfallstation des Universitätsspitals Basel (USB) auf, weil sie sich seit ihrer Rückkehr aus Afrika nicht wohl fühlt, leicht fiebrig ist und aus ihr nicht nachvollziehbaren Gründen an Gewicht verloren hat. Die Ärzte machen einige Tests, und es erhärtet sich aufgrund des gemachten Tuberkulintests der Verdacht, dass die Frau an Tuberkulose leidet. Um die Diagnose sicher bestätigen zu können, wird für den nächsten Tag ein CT der Lunge angeordnet. Das CT bestätigt die Diagnose Tuberkulose, zudem zeigt es Indizien für Lungenkrebs. Die Frau wird hospitalisiert, es wird ihr Antibiotika gegen die Tuberkulose verabreicht und es werden weitere Untersuchungen bezüglich des indizierten Lungenkrebses vorgenommen. Auch dieser wird nach gründlicher Untersuchung bestätigt. Da der Tumor noch keine Metastasen gebildet hat und die Antibiotikatherapie gut anschlägt, wird das Karzinom einige Tage darauf operativ entfernt. Die nachfolgenden Untersuchungen werden auf Wunsch der Frau vom Hausarzt durchgeführt. Die Patientin ist bei der Krankenversicherung ÖKK allgemein versichert.

### 1 Datenfluss im USB

#### 1.1 *Klinikinformationssystem und Krankengeschichte*

Beim Eintritt der Patientin in die Notfallstation werden ihre Personalien (*Name, Adresse, Geburtsdatum, aber auch Krankenkasse und Versichertennummer* sowie sog. *fakultative Angaben*) ins hauseigene Klinikinformationssystem (KIS) aufgenommen und es wird ein Falldossier, sog. Krankengeschichte (KG), für sie eröffnet, welches sämtliche behandlungsrelevanten Daten (u.a. *Diagnosen, die angeordneten Massnahmen, Befunde, Medikation, aber auch Angaben zum Privatleben wie Zivilstand, Kinder, Arbeit*), die bei der weiteren Untersuchung und Behandlung anfallen werden, festhält. Als Rechtfertigung für diese Datenbearbeitung gilt § 3 Abs. 1 ÖspG und § 29 GesG; die Frau wird weder um Einwilligung zur Aufnahme ihrer Daten ins KIS gebeten, noch kann sie das Anlegen eines Dossiers verhindern. Einzig über die Bekannt-

gabe der sog. fakultativen Angaben kann sie selbst entscheiden. Zugang zu den Daten im KIS und der KG haben all jene Personen, die diese für ihre Aufgabenerfüllung benötigen, also die entsprechenden Ärzte, das Pflegepersonal, aber auch die Labormitarbeitenden, die Codierstelle und die Administration, welche die Daten an die entsprechenden externen Stellen meldet. Aber auch weitere Personen, wie beispielsweise Leute von der IT, können möglicherweise Zugang zu diesen Daten haben, wenn es für ihre Aufgabenerfüllung nötig ist, beispielsweise für die Administration und Organisation der EDV-Systeme.

### 1.2 *Seelsorger*

Während ihres Aufenthaltes im Spital wird die Frau vom hauseigenen Spitalseelsorger besucht, der ihr seine Unterstützung anbietet. Der Seelsorger hat die Daten der Frau aus einer Liste, welche das USB den hauseigenen Spitalseelsorgern gestützt auf § 8 Abs. 2 Spitalseelsorgevertrag<sup>508</sup> täglich zukommen lässt. Nachdem die Frau die Unterstützung des Seelsorgers gerne angenommen hat, notiert sich dieser *Namen, Krankheit und Gesprächsinhalt*, so dass er in Anbetracht seiner zahlreichen Kunden den Überblick behalten kann. Diese Daten legt er in einer eigenen Datenablage ab, zu der nur er selbst Zugang hat.

### 1.3 *Studie*

Noch vor der Operation tritt der behandelnde Arzt an die Frau heran und erklärt ihr, dass er Leiter einer schweizweiten Studie sei, welche den Einfluss von Umweltfaktoren auf die Bildung von Lungenkrebs erforsche. Nachdem sie der Arzt über alle Einzelheiten der Studie informiert hat, gibt die Patientin ihre Einwilligung zur Studienteilnahme nach Art. 16 f. HFG. Noch am selben Tag erhält sie Besuch einer Forscherin, welche ihr die verschiedensten Fragen stellt. Die gewonnenen Daten (u.a. *Name, Kontaktangaben, Geschlecht, Alter, Angaben über die täglichen Gewohnheiten be-*

---

<sup>508</sup> Vertrag vom 1. November 2012 über die Seelsorge in den öffentlichen Spitälern zwischen dem Universitätsspital, Felix Platter-Spital und den Universitären Psychiatrischen Kliniken einerseits, nachfolgend öffentliche Spitäler und der Evangelisch-reformierten Kirche Basel-Stadt, der Römisch-katholischen Kirche Basel-Stadt, der Christkatholischen Kirche Basel-Stadt und der Israelitischen Gemeinde Basel andererseits.

*züglich Ernährung, Suchtmittelkonsum, aber auch zur körperlichen Betätigung, Arbeitslast und persönlichen Beziehungen*) werden in die hauseigenen Studiendatenbank eingepflegt, anstelle des Namens wird jedoch eine eindeutige Identifikationsnummer verwendet. Der Name und der Schlüssel zur Reidentifikation werden in einer separaten Datenbank gespeichert. Zugang zu ihren pseudonymisierten Studiendaten erhalten alle mit dieser Forschung betrauten Personen. Zugang zur Namensdatenbank erhalten nur der Studienleiter sowie jene Personen, die für das Matching zuständig sind. Die von der Patientin erhobenen Daten können mit ihrer Einwilligung auch für weitere Forschungszwecke verwendet werden. Wenn die Daten pseudonymisiert, d.h. nach HFG verschlüsselt wurden, steht ihr ein Widerspruchsrecht zu (Art. 33 HFG). Nur wenn es unmöglich oder unverhältnismässig schwierig ist, die Einwilligung einzuholen beziehungsweise über das Widerspruchsrecht zu informieren, oder wenn davon ausgegangen wird, dass es der Frau nicht zugemutet werden kann, mit ihrer Krankheit erneut in Kontakt zu treten, kann auf die Einwilligung bzw. die Information über das Widerspruchsrecht verzichtet werden, sofern sie keine diesbezügliche Ablehnung je dokumentiert hat und das Forschungsinteresse an den Daten überwiegt (Art. 34 HFG). Wurden die Daten jedoch anonymisiert, so ist das HFG nicht mehr anwendbar (Art. 2 Abs. 2 lit. c HFG), was bedeutet, dass es in diesem Falle keiner Einwilligung oder Information bezüglich der forschungsbezogenen Wiederverwendung bedarf. Wer im Rahmen der weiteren Forschungszwecke Zugriff auf die Daten hat, hängt deshalb nebst dem individuellen Setting vom Grad des Personenbezuges ab und ist im Vornherein nur schwer abzuschätzen.

## 2 Datenfluss an Externe

### 2.1 Nachbehandelnder Arzt

Damit die Frau nach ihrer Spitalentlassung die von ihr benötigte medizinische Versorgung erhält, stellt das USB für den nachbehandelnden Arzt einen sog. Austrittsbericht aus. Dieser enthält in erster Linie *Angaben betreffend die Diagnosen und Nebendiagnosen, die Beurteilung und Verlauf der Krankheit, die im Spital angewandte Therapie sowie Informationen betreffend Art und Dosis der bei Austritt verordneten Arzneimittel*. § 27 Abs. 2 GesG sieht vor, dass die Einwilligung der Patientin zur Bekanntgabe dieser Daten an den nachbehandelnden Arzt vermutet wird, was bedeu-

tet, dass der Austrittsbericht nur dann nicht an den nachbehandelnden Arzt geschickt wird, wenn die Patientin sich explizit dagegen wehrt. Zugang zu diesen Daten haben in der Regel der nachbehandelnde Arzt und seine Praxisgehilfen, die diese Dokumente in einer weiteren KG ablegen.

### **2.2 Krankenkasse**

Das USB stellt der ÖKK für die Überprüfung der Berechnung der Vergütung sowie der Wirtschaftlichkeit der erbrachten Leistungen eine detaillierte Rechnung aus, welche *das Kalendarium der Behandlungen, die erbrachten Leistungen, Haupt- und Nebendiagnosen sowie Prozeduren, die zur Berechnung des anwendbaren Tarifs notwendig sind, Kennnummer der Versichertenkarte sowie die AHV-Nummer* enthält (Art. 59 Abs. 1 KVV). Die Rechnung sowie die Datensätze mit den administrativen und medizinischen Angaben werden vom USB ausschliesslich an die zertifizierte Datenannahmestelle des Versicherers (Dispatcher Centris) versandt, welche sodann bestimmt, dass für die vorliegende Rechnung eine weitere Prüfung benötigt wird (Art. 59a Abs. 3 und 4 KVV). Die Datenannahmestelle leitet die dazu notwendigen Angaben an die ÖKK zur vertieften Überprüfung weiter (Art. 59a Abs. 4 KVV), woraufhin der zuständige Sachbearbeiter mit dem USB Kontakt aufnimmt und *weitere Daten, wie Operations- und Austrittsbericht*, anfordert (Art. 42 Abs. 4 KVG). Da das USB in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet ist, medizinische Angaben nur dem Vertrauensarzt der ÖKK bekannt zu geben (Art. 57 KVG), wird die Patientin über ihr Recht informiert. Die Patientin besteht darauf, die Zusatzdaten nur dem Vertrauensarzt der ÖKK zu übermitteln. Das USB sendet die angeforderten Daten deshalb nun direkt an den Vertrauensarzt, welcher die Rechnung erneut prüft und zur Zahlung freigibt. Wie aufgezeigt basieren sämtliche Datenbearbeitungsvorgänge auf einer Rechtsgrundlage; die Einwilligung der Patientin ist nicht vonnöten. Zugriff auf die Daten aus der Intimsphäre haben nur der Vertrauensarzt und die Datenannahmestelle. Auf alle übrigen Daten können auch die anderen Abteilungen zugreifen (Details siehe Tabelle 1).



### Exkurs

#### Datenverarbeitungssysteme am Beispiel der ÖKK-Krankenpflegeversicherung

Bei den meisten in dieser Praxisstudie vorgestellten Datenempfänger und Wiederbekanntgeber läuft die Verarbeitung der erhaltenen Daten über EDV-Systeme, welche nicht von den eigentlichen Datenempfängern, sondern von externen Privatunternehmen betrieben werden. Eine solche Auslagerung des EDV-Betriebes und der damit verbundenen Datenbekanntgabe an die Mitarbeitenden solcher Privatunternehmen ist nicht per se unzulässig, es bedeutet jedoch, dass der Umgang mit den Daten nicht im gleichen Masse kontrolliert werden kann und wird, wie wenn die Datenverarbeitung inhouse stattfindet. Es bedeutet aber auch, dass der Kreis der Zugangsberechtigten zu den sensiblen Gesundheitsdaten in der Regel viel mehr Menschen umfasst, als dies von der betroffenen Person abgeschätzt werden kann, und dass diese Personen zwar vertraglich an die Verschwiegenheit bezüglich der zur Kenntnis gebrachten Daten verpflichtet werden können, eine Überbindung des strafrechtlich geahndeten Arztgeheimnisses wohl aber nicht in Frage kommt.<sup>509</sup> Die folgenden Daten aus dem ÖKK-Bearbeitungsreglement über die Datenannahmestelle<sup>510</sup> und dem Bearbeitungsreglement ÖKK-Informationssystem<sup>511</sup> sollen exemplarisch für die anderen Datenempfänger und Wiederbekanntgeber aufzeigen, wie die Datenverarbeitung bei einer solchen Stelle aussehen kann, wer dabei involviert sein kann, wie viele Personen Zugriff auf die Personendaten erhalten können und wie viele weitere Empfänger mit diesen Daten bedient werden können.

---

<sup>509</sup> SCHWANINGER/LATTMANN, RZ 24 ff.

<sup>510</sup> Bearbeitungsreglement ÖKK-Informationssystem Datenannahmestelle vom 16. April 2013 (Bearbeitungsreglement 1), gefunden auf: <[https://www.oekk.ch/de/Portaldata/1/Resources/ueberoekk/\\_pdf/Bearbeitungsreglement\\_Datenannahmestelle.pdf](https://www.oekk.ch/de/Portaldata/1/Resources/ueberoekk/_pdf/Bearbeitungsreglement_Datenannahmestelle.pdf)> (zuletzt besucht am 16.10.2014).

<sup>511</sup> Bearbeitungsreglement ÖKK-Informationssystem Versicherungswesen vom 16. September 2013 (Bearbeitungsreglement 2), gefunden auf: <[https://www.oekk.ch/Portaldata/1/Resources/ueberoekk/\\_pdf/Bearbeitungsreglement\\_Versicherungswesen.pdf](https://www.oekk.ch/Portaldata/1/Resources/ueberoekk/_pdf/Bearbeitungsreglement_Versicherungswesen.pdf)> (zuletzt besucht am 16.10.2014).

### **Das ÖKK-Informationssystem**

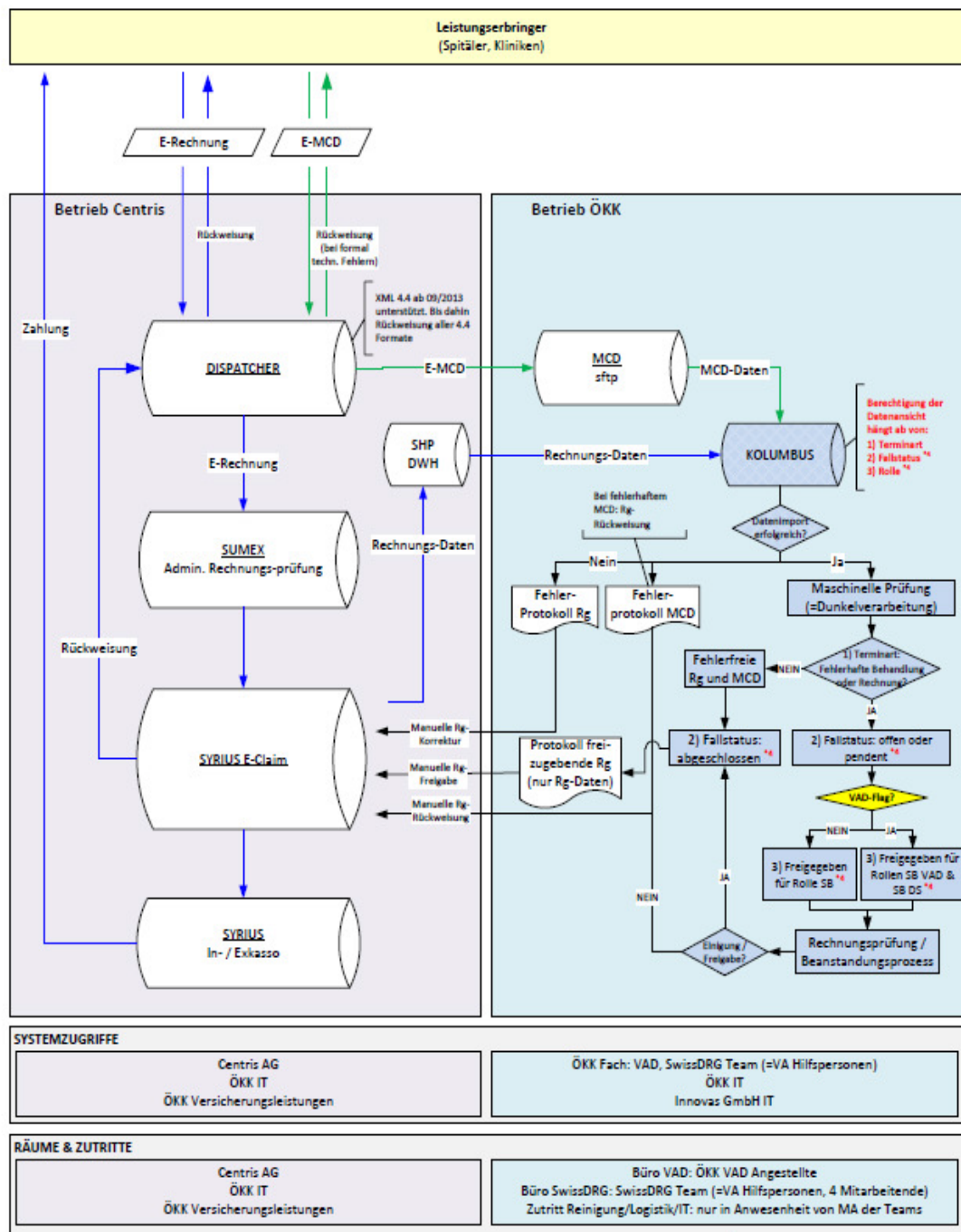
Das ÖKK-Informationssystem DAS beinhaltet zwei Subsysteme (Syrius und Kolumbus). Während in Syrius als Kernapplikation die Administration von Kundendaten (Adressmutationen, Kontomutationen, Deckungsänderung) sowie die Leistungsverarbeitung erfolgt, stellt Kolumbus ein elektronisches Prüfsystem für die SwissDRG-Rechnungen dar, welche die fachliche (medizinisch/tarifarisch) sowie die Kostenprüfung vornimmt und ein Expertensystem mit Optimierungsvorschlägen für Behandlungen enthält.

## VII Praxisstudie

### Subsystemübersicht:<sup>512</sup>

Scope DAS: Leistungsprozess stationäre SwissDRG Rechnungen

11.09.2013



<sup>512</sup> S. 15 Bearbeitungsreglement 1.

## VII Praxisstudie

Nicht abschliessende Liste der Anzahl Mitarbeitenden pro Organisationseinheit, welche Zugriff auf die einzelnen Subsysteme haben (Tabelle 1):<sup>513</sup>

Subsystem	Organisationseinheit	Welche Datenkategorien ÖKK werden bearbeitet?	MA
Syrius	Alle Abteilungen mit Kundenkontakt	Name/Adresse/Tel, Geburtsdatum, Familienverhältnisse, Nationalität, AHV-Nummer, Gesetzliche Vertretung, Angehörige,	395
	ÖKK Informatik	Angaben zur Behinderung, Gesundheit, Massnahmen der sozialen Hilfe	9
	Centris AG		9
Kolumbus	VA	Name/Adresse/Tel, Geburtsdatum, Familienverhältnisse, Nationalität, AHV-Nummer, Gesundheit, Intimsphäre, Massnahmen der sozialen Hilfe	3
	DAS		4

(in der Tabelle wird nicht aufgezeigt, wie viele Mitarbeitende gemäss Zugriffsberechtigung tatsächlich Zugang zu den einzelnen Datenkategorien haben)

Liste der weiteren Datenempfänger (Tabelle 2):<sup>514</sup>

	Empfänger	Datenart ÖKK	Zweck	Periodizität	Medium	Rechtsgrundlage
Syrius	<ul style="list-style-type: none"> <li>• Sanacare (Arztpraxis)</li> <li>• Centramed (Arztpraxen)</li> <li>• RVK</li> <li>• Veka-Zentrum</li> <li>Versichertenkarte (Prüfung der Versicherungsdeckung)</li> <li>• Cent (Stammdaten Rechnungsscanning)</li> <li>• Medgate (Telemedizin)</li> <li>• Postfinance (Auszahlungen, DD)</li> <li>• SIX (LSV)</li> <li>• MediData (ERrechnungen)</li> <li>• EOS (Überwachung und Erstellung von Betriebsdokumenten)</li> <li>• ZMV (Zentrale Meldestelle für Versicherungsverwechsel)</li> <li>• Kantone (Individuelle Prämienverbilligung)</li> </ul>	Stammdaten, Leistungsdaten, Prämiendaten, Mahnungen, Kostengutsprachen Deckungsdaten	Leistungserbringung gemäss Vertrag	Nach Bedarf	Papier oder elektronisch	KVG 84 (Bearbeiter);  KVG 84a I lit. a (Leistungserbringer)  DL-Vertrag mit Centris

<sup>513</sup> S. 21 Bearbeitungsreglement 1.

<sup>514</sup> S. 34 Bearbeitungsreglement 2.

### **2.3 Bereich Gesundheitsversorgung des Gesundheitsdepartements Basel-Stadt**

Da der Wohnkanton der Patientin sich bei stationär erbrachten Leistungen in seinen Listenspitälern zu mindestens 55% an den Kosten beteiligen muss (Art. 49a KVG), schickt das USB dem Gesundheitsdepartement des Kantons Basel-Stadt – als Vertreter für den Kanton in diesen Angelegenheiten – ebenfalls eine Rechnung. Diese erfolgt monatlich oder quartalsweise in einer Sammelrechnung und beinhaltet *Name, Vorname, Adresse, Geburtsdatum, Fallbeginn, Fallende, Anzahl Tage, DRG-Code, Bereich (z.B. Psychiatrie oder Akutsomatik), Kostengewicht Soll/Kostengewicht Ist/Baserate oder anderer Tarif, falls noch kein DRG besteht, Totalbetrag, Klasse (allgemein, halbprivat oder privat), Krankenversicherung, Kostenanteil Krankenkasse, Kostenanteil Kanton.*

Das Gesundheitsdepartement prüft die Rechnungsdaten. Insbesondere wird eine formale Kontrolle (Doppelrechnungen, stornierte Fälle, Berechnungsfehler), eine Tarifkontrolle (korrektes Kostengewicht, korrekte Baserate, korrekter Kostenverteiler) sowie eine Wohnsitzkontrolle durchgeführt. Für Letztere findet ein Abgleich mit dem kantonalen Datenmarkt statt. Zugang zu den Daten erhalten nur die für die Abrechnung zuständigen Mitarbeitenden des Gesundheitsdepartements. Die für die Zahlung relevanten Daten werden sodann ohne personenbezogene Daten, dafür mit einer eindeutigen ID, an die Zahlungsschnittstelle übermittelt, die die Zahlung veranlasst.

### **2.4 Kantonsarzt**

Des Weiteren erstattet der fallführende Arzt des USB dem Kantonsarzt Meldung über den Fall seiner Patientin, da Tuberkulose eine jener übertragbaren Krankheiten ist, die nach Art. 27 Abs. 1 lit. a EpG i.V.m. Art. 4 Melde-VO vom Spital an den Kantonsarzt jenes Kantons zu melden sind, in dem die untersuchte Person Wohnsitz hat. Da es sich im vorliegenden Fall um eine Erstmeldung von Tuberkulose handelt, müssen nebst den *meldepflichtigen Beobachtungen* und den *ersten epidemiologischen Angaben der Name* sowie *die Adresse und Telefonnummer, das Geschlecht, das Geburtsdatum* und *den Wohnort der Patientin* gemeldet werden. Ausserdem holt der Kantonsarzt nach einer Woche beim behandelnden Arzt eine Ergänzungsmeldung

zur Abschätzung des Handlungsbedarfes und für erweiterte epidemiologische Angaben ein, welche *zusätzliche Daten zur Exposition, dem Krankheitsverlauf sowie den getroffenen Massnahmen ein*,<sup>515</sup> aber auch *die Nationalität und der Beruf*, wenn er epidemiologisch wichtig ist, müssen gemeldet werden (Art. 7 Melde-VO i.V.m. Anhang 4 der VO des EDI über Arzt- und Labormeldungen).

Der Kantonsarzt leitet die Meldung dem BAG weiter (Art. 27 Abs. 1 lit. a EpG). Dieses ist darüber hinaus befugt, den mit der Behandlung übertragbarer Krankheiten beauftragten Ärzten, den Kantonsärzten und anderen mit Gesundheitsaufgaben beauftragten Behörden sowie in- und ausländischen Institutionen des Gesundheitswesens die Daten bekannt zu geben (Art. 27 Abs. 2 EpG).<sup>516</sup> Wer Zugang zu diesen Personendaten hat, lässt sich aufgrund des breitgefächerten Adressatenkreis nicht eruieren. Er kann maximal mit all jenen Personen, die mit der Bekämpfung und Behandlung von übertragbaren Krankheiten beauftragt sind, umschrieben werden. Als Rechtfertigung für die diversen Datenflüsse sind auch hier wieder die einschlägigen Rechtsgrundlagen zu nennen.

---

<sup>515</sup> Es kann davon ausgegangen werden, dass es sich hierbei um die neu in Art. 59 und 62 nEpG genannten Daten handelt, also *Name, Vorname, Adresse, Geburtsdatum, berufliche Tätigkeit, Angaben über Reisewege, Aufenthaltsorte und Kontakte mit Personen, Tieren und Gegenständen, Ergebnisse von medizinischen Untersuchungen. und epidemiologischen Abklärungen, Angaben über die Zugehörigkeit zu einer bestimmten Risikogruppe sowie zu Massnahmen zur Verhütung und Bekämpfung der Krankheit.* (Botschaft über die Schaffung und die Anpassung gesetzlicher Grundlagen, S. 9017 f.).

<sup>516</sup> 2016 soll das revidierte EpG und die dazugehörenden Verordnungen in Kraft treten. An der Meldepflicht für Ärzte beim Befund Tuberkulose ändert sich dadurch nicht viel. Innerhalb einer Woche muss der behandelnde Arzt dem Kantonsarzt nebst den *Angaben zur meldepflichtigen Beobachtung Name, Vorname, Adresse, Telefonnummer, gegebenenfalls Aufenthaltsort Geschlecht, Geburtsdatum, Staatsangehörigkeit, berufliche Tätigkeit*, neu aber auch, *Herkunftsland und Aufenthaltsstatus* melden (Art. 2 i.V.m. Anhang 1 des Entwurfs vom 7. Juli 2014 der Verordnung des EDI über die meldepflichtigen Beobachtungen übertragbarer Krankheiten des Menschen). Eine diese Angaben bezügliche Ergänzungsmeldung ist vorgesehen bei Behandlungsabschluss oder -abbruch (Anhang 1 des Entwurfs vom 7. Juli 2014 der Verordnung des EDI über die meldepflichtigen Beobachtungen übertragbarer Krankheiten des Menschen). Auch das revidierte EpG sieht die Bekanntgabeermächtigung des BAG an Kantonsärzte und andere in- und ausländische Behörden vor, sofern die Datenbekanntgabe der Verhütung oder Bekämpfung übertragbarer Krankheiten dient (Art. 59 und 62 nEpG).

## 2.5 Krebsregister beider Basel

Der behandelnde Arzt unterrichtet die Patientin über die Möglichkeit der Aufnahme ihrer Tumorerkrankung im Krebsregister beider Basel (KRBB), welches unter anderem zum Ziel hat, die Krebsursachenforschung voranzutreiben. Die Frau gibt ihre Einwilligung zur Bekanntgabe, woraufhin der Arzt ihren Tumor beim KRBB registrieren lässt. Da es sich um einen neuen Fall handelt, erhält der Arzt einen Malignom-Fragenbogen, welchen er an das KRBB zurück schicken muss; das KRBB selbst hat keinen Patientenkontakt. Rechtsgrundlage für das Datenbearbeiten durch das KRBB ist die seit 1995 bestehende generelle Registerbewilligung der Eidgenössischen Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung nach Artikel 321<sup>bis</sup> StGB, welche zur Entgegennahme nicht anonymisierter Daten ermächtigt.<sup>517</sup> Im Register selbst werden die Daten sodann anonymisiert und nur in anonymisierter Form bearbeitet, so dass die Identifikation eines Patienten nicht möglich ist.<sup>518</sup> Zugang zu diesen Daten haben sicherlich die sechs Krebsregistermitarbeitenden, evt. auch der IT-Verantwortliche, sofern er dies für seine Aufgabenerfüllung bedarf.<sup>519</sup>

---

<sup>517</sup> <<http://www.gesundheitsdienste.bs.ch/ueber-uns/organisation/abteilung-medizinisch-pharmazeutische-dienste/krebsregister.html>> (zuletzt besucht am 15.10.2014).

<sup>518</sup> BBl 1995 III 311 ff.

<sup>519</sup> Derzeit ist der Bund daran, die Krebsregistrierung zu harmonisieren. Der Vorentwurf eines Bundesgesetzes über die Krebsregistrierung (VE KRG)<sup>519</sup> sieht u.a. für jede Krebserkrankung eine Meldung verschiedenster Daten (Name, AHV-Nummer, Adresse, Geburtsdatum, Geburtsort, Geschlecht, Zivilstand, Staatsangehörigkeit, Datum und Grundlage der diagnostischen Untersuchung, diagnostische Angaben zur Krebserkrankung, Art, Ort und Beginn der Erstbehandlung) an das kantonale Krebsregister vor (Art. 4 Abs. 1 VE KRG). Die betroffenen Personen haben diesbezüglich ein Widerspruchsrecht (Art. 4 Abs. 4 VE KRG), allerdings können auch die Daten der widersprechenden Personen aufgrund eines Abgleichs mit der Todesursachenstatistik des Bundesamtes für Statistik dorthin fließen (Art. 11 VE KRG). Der Bundesrat kann die Erhebung weiterer Daten, insbesondere zum Krankheitsverlauf, Behandlungsverlauf, aber auch zu den Lebensumständen und der Lebensqualität mit Einwilligung der Patienten vorsehen (Art. 5 VE KRG). Die vom kantonalen Krebsregister erfassten Daten sollen sodann von einer Vertrauensstelle pseudonymisiert werden und so an eine nationale Krebsregistrierungsstelle weiter geleitet werden (Art. 12 VE KRG). Die durch diese aufbereiteten Daten werden von der Vertrauensstelle wieder entpseudonymisiert und dergleichen dem Bundesamt für Statistik weiter geleitet (Art. 15 VE KRG).

## **2.6 Staatsarchiv Basel-Stadt**

Das USB ist ebenfalls verpflichtet, Unterlagen, welche es zur Aufgabenerfüllung nicht mehr braucht, auszusondern und periodisch dem Staatsarchiv zur Übernahme anzubieten. Anzubieten sind auch Unterlagen, die schutzwürdige Personendaten enthalten oder/und einer besonderen Geheimhaltungspflicht unterstehen (§ 7 Abs. 1 ArchivG), was beides auf die komplette KG der Patientin zutrifft. Zugang zu diesen Daten haben vorerst nur die Mitarbeitenden des Staatsarchives. 10 Jahre nach dem Tod der Patientin – oder, falls dieser nicht eruiert werden kann, 100 Jahre ihrer Geburt – werden diese Daten der Öffentlichkeit zugänglich gemacht (§ 10 Abs. 2 ArchivG), wobei unter Umständen die Schutzfrist verlängert oder verkürzt werden kann (§ 10 Abs. 4 ff. ArchivG). Auch dieser Datenfluss beruht auf einer Rechtsgrundlage, ein Veto der Patientin würde keine Wirkung erzeugen.

## **2.7 Zentrale Statistikstelle Basel-Stadt**

Es kann auch sein, dass das USB Daten der Patientin der zentrale Statistikstelle bekannt geben muss. Bis anhin stützt sich diese Bekanntgabepflicht auf § 22 Abs. 3 IDG, nach Wirksamwerden des neuen Statistikgesetzes<sup>520</sup> auf § 8 Abs. 1 StatG. Ob und welche Daten bekannt gegeben werden müssen, hängt dann vom Regierungsrat zu verabschiedenden Statistikprogramm ab (§ 11 StatG). Die erhobenen Daten werden von der zentralen Statistikstelle für die weitere statistische Auswertung umgehend pseudonymisiert (§ 13 StatG). Zugang zu diesen Rohdaten haben die Mitarbeitenden der zentralen Statistikstelle; die pseudonymisierten Daten können jedoch ohne Pseudonymschlüssel an andere öffentliche Statistikstellen und an Forschungsstellen zu statistischen Zwecken weitergegeben werden (§ 17 StatG). Hierzu gehört auch die Datenbekanntgabe an das Bundesamt für Statistik, wobei dieses die Daten auch direkt beim USB einfordern könnte (Art. 4 Abs. 2 BStatG). Der Kreis der Zugangsberechtigten bezüglich der Rohdaten kann wohl nur mit den Mitarbeitenden der zentralen Statistikstelle und des Bundesamtes für Statistik umschrieben werden.

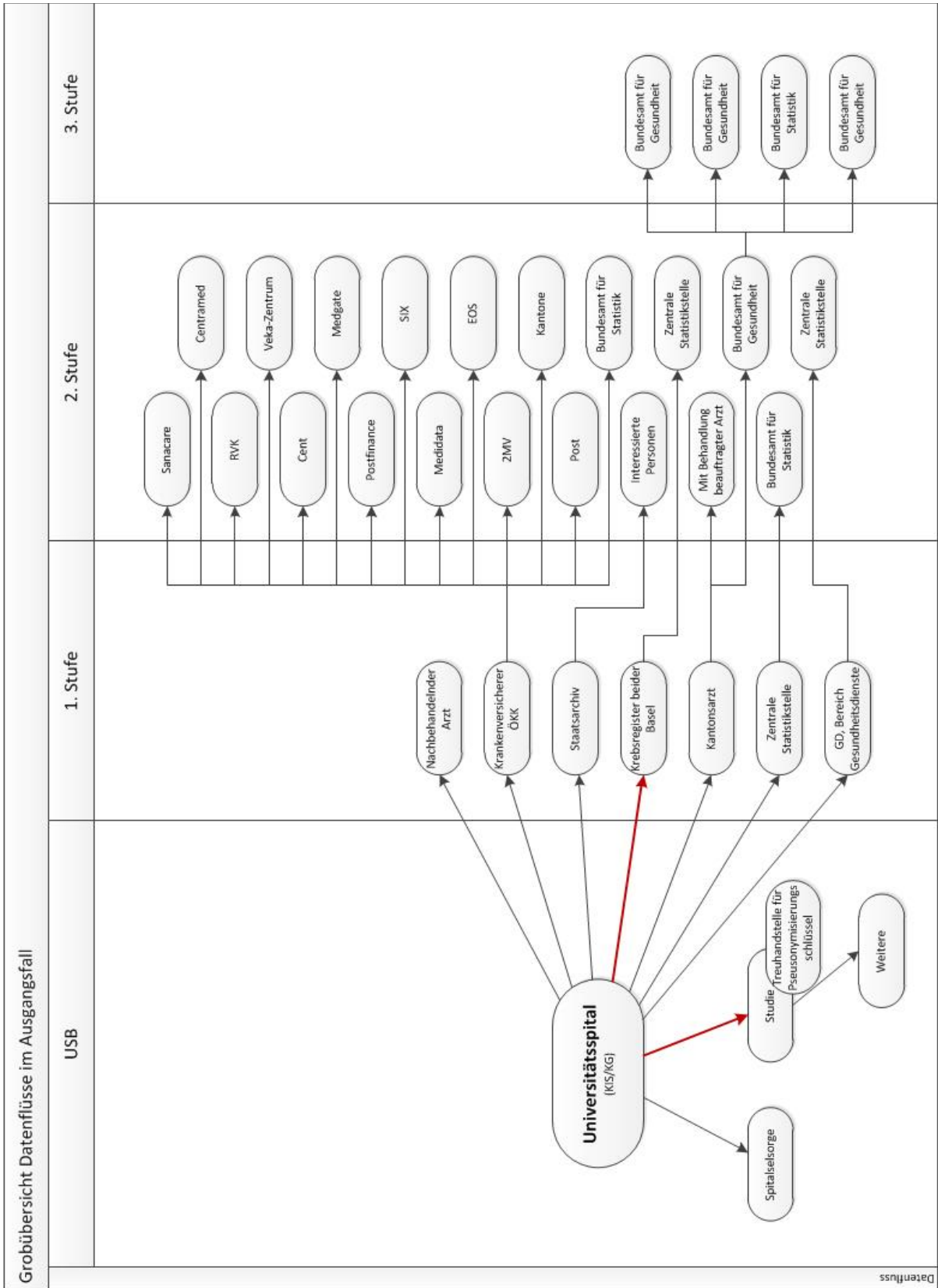
---

<sup>520</sup> Der Grosse Rat des Kantons Basel-Stadt hat am 21. Mai 2014 das kantonale Gesetz über die öffentliche Statistik (StatG) beschlossen <<http://www.grosserrat.bs.ch/dokumente/100378/000000378086.pdf>> (zuletzt besucht am 31.12.2014).



## **2.8    *Übersicht über die beschriebenen Datenflüsse***

Die folgende Übersicht über die vorne beschriebenen Datenflüsse zeigt, dass gerade zwei dieser Datenflüsse (vom USB zur ÖKK und vom USB zum Krebsregister beider Basel) ausschliesslich durch die Einwilligung legitimiert sind. Alle anderen Datenflüsse sind durch eine Rechtsgrundlage gerechtfertigt, wobei die betroffenen Personen bei der Bekanntgabe an den nachbehandelnden Arzt die gesetzliche Vermutung umstossen können.



### 3 Résumé

Die vorliegende Praxisstudie hat gezeigt, dass im Rahmen der öffentlichen Gesundheitsversorgung viele Bereiche vom Staat geregelt sind und sich die Datenflüsse überwiegend auf eine rechtliche Grundlage stützen. Jeder Datenfluss hat durchaus seine Berechtigung, doch zeigt dieses Beispiel gut, dass die Regelungsdichte im Gesundheitsbereich bereits so hoch ist, dass man sich fragen muss, ob das Grundrecht auf informationelle Selbstbestimmung hier nicht quasi bereits durch die Hintertür ausgehöhlt wurde.<sup>521</sup> Allein im Rahmen dieses Fallbeispiels wurden unzählige Daten erhoben und über zwanzig Stellen waren involviert. Etwas anders mag es im Rahmen der privatrechtlichen Gesundheitsversorgung aussehen, wenn der Patient sich etwa vom Hausarzt oder vom Zahnarzt behandelt lässt. In diesen Fällen kann er einen gewissen Einfluss auf die Datenflüsse ausüben. Doch sobald eine Abrechnung über die obligatorische Krankenkasse vorgesehen ist, diktiert das KVG, welche Daten wie und wohin bekannt gegeben werden müssen, womit die ganzen von den Krankenkassen ausgehenden Datenflüsse wieder zum Tragen kommen. Dies gilt im Übrigen, einfach mit anderen Rechtsgrundlagen, auch für Abrechnungen über die Zusatzversicherungen, die Invalidenversicherung und die Unfallversicherung. Darüber hinaus kann das kantonale Recht auch für privat praktizierende Ärzte Datenbearbeitungsvorschriften vorsehen. So normiert etwa § 29 GesG eine Dokumentationspflicht für *alle* Fachpersonen im Gesundheitsbereich.

Insoweit kann festgehalten werden, dass auch mit einer Stärkung des informationellen Selbstbestimmungsrechts die vom Gesetzgeber als notwendig erachteten Datenbearbeitungen grundsätzlich möglich sind und es hier nicht etwa zum gefürchteten Informationsengpass<sup>522</sup> kommt. Es ist aber auch festzuhalten, dass der informationellen Selbstbestimmung im Gesundheitsbereich nur noch wenig Raum bleibt, vielleicht zu wenig. Denn auch wenn konkrete Informationsbedürfnisse den Erlass von Rechtsgrundlagen als Rechtfertigungsgründe für den Grundrechtseingriff legitimieren, ist der Wert, der für die Betroffenen auf dem Spiel steht, zumindest auch aus genereller Sicht zu würdigen: Ein einzelner Fall übergangener Autonomie mag noch

---

<sup>521</sup> Zur Gefahr der Aushöhlung des Grundrechtsschutzes siehe Kapitel IV, Ziffer 3.

<sup>522</sup> Zur Kritik eines Informationsverbots siehe Kapitel IV, Ziffer 3.

## VII Praxisstudie

nicht schwer wiegen, deren Kumulation führt allerdings zur Erosion des Grundrechtsschutzes schlechthin.<sup>523</sup>

---

<sup>523</sup> Vgl. DRUEY, Strukturelle Schwächen, S. 146.

## VIII Schlusswort

BELSER hat die Frage aufgeworfen, weshalb ein umfassendes Selbstbestimmungsrecht die bessere Antwort des Rechts auf die Gefahren für die Freiheit des Einzelnen und des Gemeinwohls, welche durch die moderne Datenbearbeitung entstehen, sein soll als klare Verbote, Regeln, Einsichts- und Kontrollrechte sowie die Aufsicht.<sup>524</sup> Die Antwort darauf ist nach den gemachten Erläuterungen klar: weil solche Verbote, Regeln, Einsichts- und Kontrollrechte nicht reichen. Es geht eben nicht «einfach» nur um den Schutz irgendwelcher persönlicher Daten und Informationen, sondern es geht letztlich um die Grundvoraussetzung für eine freiheitsorientierte Gesellschaft, welche auf selbstbestimmten Individuen fusst. Damit der einzelne zu einem solch selbstbestimmten Individuum werden kann, braucht er einen privaten «Raum», in dem er sich selbst und das Bild, welches er nach aussen abgibt, frei entwickeln darf und somit seine sozialen Rollen und Beziehungen regulieren kann. Dieser «Raum» ist die Privatheit, gemäss SOFSKY die «Zitadelle der persönlichen Freiheit.»<sup>525</sup> Ihre Verteidigung geht deutlich über den Datenschutz hinaus – sie ist Aufgabe jeder Zivilisation.<sup>526</sup> Die Privatheit kann allerdings nur dann Bestand haben, wenn der einzelne über den Umgang mit den ihn betreffenden Daten und Informationen zumindest mitentscheiden kann und nicht bloss im Sinne eines stillen Teilhabers nur über die Vorgänge informiert wird. Insoweit ist die informationelle Selbstbestimmung unmittelbare Voraussetzung für die Privatheit und als solche unmittelbare Voraussetzung für die Entfaltung freier Individuen und eines darauf basierenden Staates. Die vorliegende Dissertation vermochte die besagten Zusammenhänge aufzuzeigen, obwohl zum Teil berechnete Kritik an deren Realisierbarkeit besteht. Es ist deshalb am Gesetzgeber, aber auch an der Rechtsprechung, dafür zu sorgen, dass die Bedingungen für eine effektive Durchsetzung dieses elementaren Rechtes geschaffen werden. Immerhin hat die Staatspolitische Kommission des Nationalrates den Handlungsbedarf erkannt, denn sie möchte ein neues Grundrecht auf informationelle Selbstbestimmung

---

<sup>524</sup> BELSER, Instrumente, S. 26.

<sup>525</sup> SOFSKY, S. 37.

<sup>526</sup> SOFSKY, S. 28.

## VIII Schlusswort

festschreiben. Damit hat sie einer parlamentarischen Initiative Folge gegeben, welche die Bundesverfassung in diesem Sinne ändern will. In Anbetracht einer zunehmend digitalisierten Welt erachte es die Kommission für angezeigt, dass das Recht auf informationelle Selbstbestimmung explizit als persönliches Freiheitsrecht anerkannt werde. Dieser Paradigmenwechsel führe im Ergebnis zu einer Beweislastumkehr zu Lasten von Staat und kommerziellen Unternehmen und zu Gunsten der Bürgerinnen und Bürger.<sup>527</sup> Ob alleine durch die Schaffung eines expliziten Grundrechts auf informationelle Selbstbestimmung die aufgezeigten Schwierigkeiten behoben werden können, scheint fraglich, es ist aber bestimmt ein wichtiger Schritt in die richtige Richtung.

---

<sup>527</sup> <<http://www.parlament.ch/d/mm/2014/Seiten/mm-spk-n-2014-08-29.aspx>> (zuletzt besucht am 31.10.2014).

## Stichwortverzeichnis

### A

Abgrenzungsfragen .....	12
Abhören .....	26
Aktivitätsschutz .....	97
Allgemeine Handlungsfreiheit .....	44, 45, 46, 97
Analoge Daten .....	68, 78
Auffanggrundrecht .....	13

### B

Berufliche Schweigepflicht .....	20
Bewusstseinsveränderung .....	62, 63
Big data .....	83, 104, 118, 121, 127

### C

Copyright .....	116
-----------------	-----

### D

Datenbearbeiter .....	37
Digitale Daten .....	68, 111, 115
Digitalisierte Daten .....	111
Digitalisierung .....	78, 107
Dispositionsfreiheit .....	60, 66, 67, 68
Drittwirkung siehe auch Horizontalwirkung .....	105

### E

Echte Alternative .....	22, 59, 69
EDÖB .....	23, 125
Eigentumsgarantie .....	36, 46
Einwilligung .....	48, 121
E-Mail .....	25
Entscheidungsfreiheit .....	8, 17, 33, 35, 36, 42, 82

### F

Facebook .....	22, 49, 68, 104
Forschungsfreiheit .....	49
Freier Wille .....	57, 58, 66, 67, 69

### G

Gefährdungspotential .....	9, 85, 125
Gemeinsphäre .....	93
Gesellschaftlicher Konventionsverstoss .....	71
Google-Street-View-Entscheid .....	14, 77
Grundrechtsanalyse .....	32
Gruppenklagen .....	130

### H

Horizontalwirkung .....	51, 105, 108, 121, 125
-------------------------	------------------------

### I

Informationelle Privatheit .....	5, 71, 82
Informationsfreiheit .....	49
Informationspflicht .....	19, 22, 108
Informationsverbot .....	47
Inhaber einer Datensammlung .....	20
Integritätsschutz .....	96
Intimsphäre .....	93

### K

Kontrollverlust .....	72, 82, 96
-----------------------	------------

### L

Legalitätsprinzip .....	17, 21
-------------------------	--------

### M

Machtverschiebung .....	79, 104
Manipulierbarer Mensch .....	79, 81
Marlene Dietrich-Urteil .....	138
Massen- oder Streuschäden .....	129
Menschenbild .....	53
Minimalstandards .....	99, 102
Missbrauchsschutz .....	10, 13, 98, 99, 102

### O

Opt-in-Lösung .....	121
---------------------	-----

## Stichwortverzeichnis

### P

<i>Persönliche Freiheit</i> .....	5, 10, 17, 44, 92, 96
<i>Prinzip der praktischen Konkordanz</i> .....	50
<i>Privacy</i> .....	95
<i>Privatautonomie</i> .....	17, 106
<i>Privatsphäre</i> .....	26, 29, 30, 79, 92, 93
<i>Prozesskosten</i> .....	129, 133, 135

### Q

<i>Querschnittsgesetz</i> .....	17
---------------------------------	----

### R

<i>Rahmengesetz</i> .....	16
<i>Recht am eigenen Bild</i> .....	28, 114, 119
<i>Recht auf Vergessenwerden</i> .....	78
<i>Recht in Ruhe gelassen zu werden</i> .....	94
<i>Rechtsgrundlage</i> .....	21, 47
<i>Rechtsgrundlagen</i> .....	51
<i>Right of Publicity</i> .....	137
<i>Right to be let alone</i> .....	3

### S

<i>Sachbegriff</i> .....	110
<i>Sanktionsmittel</i> .....	126
<i>Schadenersatz</i> .....	129
<i>Schriftgeheimnis</i> .....	25

<i>Schutz der Persönlichkeit</i> .....	5, 16, 18, 31, 35, 88
<i>Schutzbedarf</i> .....	89
<i>Schutzobjekt</i> .....	34
<i>Schutzpflicht</i> .....	38
<i>Soziale Rollen</i> .....	33, 42, 72, 74
<i>Strafbestimmungen</i> .....	20, 25
<i>Streitgenossenschaft</i> .....	131, 133
<i>Summarisches Verfahren</i> .....	136
<i>Systemfehler</i> .....	23, 125, 135

### T

<i>Tagebuch-Beschluss</i> .....	40
---------------------------------	----

### U

<i>Unentgeltliche Rechtspflege</i> .....	135
--	-----

### V

<i>Verbandsklage</i> .....	131
<i>Vereinfachtes Verfahren</i> .....	136
<i>Vermögenswerte Persönlichkeitsrechte</i> .....	138
<i>Verschlossene Schrift</i> .....	25
<i>Volkzählungsurteil</i> .....	6, 81

### W

<i>Widerspruchsrecht</i> .....	19, 22, 108, 120
<i>Wortlautinterpretation</i> .....	45, 103



## **Lebenslauf**

1983 wurde ich in Basel geboren und habe dort die Schule bis 2003 besucht. Nach Erhalt der Matura legte ich ein Auszeitjahr ein, in dem ich einen Sprachaufenthalt in Florenz genoss und mir über meinen beruflichen Weg Klarheit verschaffte. Im Anschluss begann ich das Studium der Rechtswissenschaft. 2008 erhielt ich mein Bachelordiplom von der Universität Basel, drei Semester danach das Masterdiplom von der Universität Luzern.

Nach meinem Studienabschluss durfte ich als Volontärin meine ersten praktischen Erfahrungen als Juristin sammeln. Im Sommer 2011 folgte eine Festanstellung als juristische Mitarbeiterin beim Datenschutzbeauftragten des Kantons Basel-Stadt. Gleichzeitig bot mir Prof. Dr. iur. Thomas Gächter die Möglichkeit am Doktoratsprogramm «Biomedical Ethics and Law» teilzunehmen und in dessen Rahmen eine Dissertation zu verfassen. Nach erfolgreichem Abschluss des Programms konnte ich meinen Begutachtern die Dissertation Anfangs 2015 vorlegen.